FORM PTO-1390 (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER: HYAE:128

30 NOV 2001

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/980093

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/JP00/03482	31 May 2000	31 May 1999

TITLE OF INVENTION: DATA RECORDING MEDIUM AND DATA MANAGEMENT SYSTEM

APPLICANT(S) FOR DO/EO/US: Hiroshi KASHIWA

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [X] This express request to begin national examination procedures (35 U.S.C. 371(f) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. [ ] A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [ ] is transmitted herewith (required only if not transmitted by the International Bureau).
   b. [X] has been transmitted by the International Bureau.
   c. [ ] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [X] A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. [ ] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are transmitted herewith (required only if not transmitted by the International Bureau).
   b. [ ] have been transmitted by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. [ ] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [ ] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [X] A FIRST preliminary amendment.
    [ ] A SECOND or SUBSEQUENT preliminary amendment.
14. [ ] A substitute specification.
15. [ ] A change of power of attorney and/or address letter.
16. [X] Other items or information:
    International Publication Cover Page;
    International Search Report;
    Forms PCT/IB/301 304 308 332 and IPEA/409.

PLEASE ACCEPT THIS AS AUTHORIZATION TO DEBIT OR CREDIT FEES TO DEP. ACCT. 16-0331 PARKHURST & WENDEL

U.S. APPLICATION NO. (if known, see 37 CFR 1.5)	INTERNATIONAL APPLICATION NO.	JC10 Rec'd PCT/PTO 26 NOV 2001	ATTORNEY'S DOCKET NUMBER
09/980093	PCT/JP00/03482		HYAE:128

17. ☒ The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):	CALCULATIONS PTO USE ONLY
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO $1,040.00	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO $890.00	
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO $740.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) $710.00	
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 890.00
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	14 - 20 =	0	X $18.00	$
Independent claims	2 - 3 =	0	X $84.00	$
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$280.00	$
TOTAL OF ABOVE CALCULATIONS =				$ 890.00
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also by filed (Note 37 CFR 1.9, 1.27, 1.28).				$
SUBTOTAL =				$ 890.00
Processing fee of **$130.00** for furnishing the English translation later than ☐20 ☐30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$
TOTAL NATIONAL FEE =				$ 890.00
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$
TOTAL FEES ENCLOSED =				$ 890.00
			Amount to be: refunded	$
			charged	$

a. ☒ A check in the amount of $ 890.00 to cover the above fees is enclosed. CK# 14762

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 160331. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO
Roger W. Parkhurst
PARKHURST & WENDEL, L.L.P.
1421 Prince St., Ste. 210
Alexandria, VA 22314-2805
Tel: (703) 739-0220

SIGNATURE

Roger W. Parkhurst
NAME

25,177
REGISTRATION NUMBER

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Hiroshi KASHIWA

Serial No.: New Application (PCT/JP00/03482)

Filed: November 30, 2001

For: DATA RECORDING MEDIUM AND DATA MANAGEMENT SYSTEM

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination of the above-identified application, please enter the following specification changes as noted below:

IN THE SPECIFICATION:

Page 10, second full paragraph, cancel and replace with:

According to Claim 9 of the present invention, in the data recording medium as defined in any of Claims 1 to 8, the content output management part further has a cipher processing part for

performing an encryption processing according to a prescribed algorithm and performs authentication by a cipher between the data recording medium and the recording and reproduction apparatus, and suppresses reproduction of the content according to the authentication result.

Page 12, first and second paragraphs, cancel and replace with:

According to Claim 11 of the present invention, in the data management system as defined in Claim 10, the recording and reproduction apparatus has plural digital output openings, the reproduction history management circuit further records the number of paths when the content is outputted in digital format simultaneously through plural paths, and the number of paths is added by the reproduction history management circuit to restrict the number of output times, when the content is outputted in digital format through the plural paths.

According to the so-constituted data management system, in a recording and reproduction apparatus having plural digital output openings, the reproduction history management circuit records the number of plural paths and adds the number of paths to the number of output times in digital format output for restriction thereof,

whereby the number of copy times can be restricted when a reproduced content is digitally copied simultaneously employing plural digital outputs.

Page 13, second and third full paragraphs, cancel and replace with:

According to Claim 13 of the present invention, in the data management system as defined in Claim 12, the reproduction history management circuit further records the number of mismatch times of a result of the comparison, and when the content is reproduced, a previously set number of times is compared with the number of mismatch times held by the reproduction history management circuit, thereby to suppress reproduction of the content.

According to the so-constituted data management system, the number of mismatch times held by the reproduction history management circuit is compared with a prescribed value and reproduction of a content is suppressed, whereby it is possible to warn an owner of the content of an unjustified access by one other than the owner, resulting in further enhancement in content security.

Page 16, first full paragraph, cancel and replace with:

Figure 11 is a diagram illustrating a detailed process of Step A1 when the content of the data management system according to the first embodiment is reproduced.

Figure 12 is a diagram illustrating a detailed process of Step A2 when the content of the data management system according to the first embodiment is reproduced.

Page 18, fifth full paragraph, cancel and replace with:

Figure 31 is a diagram illustrating a detailed process of Step D4 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

Page 20, seventh paragraph to Page 21, paragraph continued, cancel and replace with:

Figure 1 is a diagram illustrating a conceptual constitution of a disk medium 100 as a data recording medium according to a first embodiment of the present invention. In figure 1, numeral 90 denotes a center hole, numeral 100 denotes a disk medium such as a DVD-RAM composed of polycarbon, numeral 101 denotes a semiconductor tip (reproduction history management circuit) which includes a nonvolatile semiconductor tip or the like as a storage element, numeral 102 denotes a data area, numeral 103 denotes a clipping area for fixing the disk medium 100 on an after-mentioned rotation drive, and numeral 104 denotes a TOB (Table of contents) area where management information of the data area 102 on the disk medium 100 is recorded.

Page 22, third paragraph, to Page 24, end of line 5, cancel and replace with:

The constitution of the disk medium 100 in more detail is as follows; the disk medium 100 comprises three layers as shown in figure 3(c), in which numeral 131 denotes a base material layer and numeral 132 denotes a recording layer in which contents are

recorded. In the semiconductor tip 101, pins 133 corresponding to the respective wiring 105 provided in the clipping area 103 are attached, by which the semiconductor tip 101 and the wiring 105 are connected so that power, a signal and the like are supplied to the semiconductor tip 101 as described above.

Its manufacturing method is as follows; the semiconductor tip 101 to which the pins 133 are attached is embedded in the base material layer 131 having a concave portion in a part of the clipping area 103. Then, the recording layers 132 are applied to both sides and the wiring 105 corresponding to respective pins 133 is formed in a metal pattern on the surface from which the pins 133 are protruding by masking or the like. While the disk medium 100 comprises three layers here, it may also comprise two layers with the recording medium layer on only one side.

With the above-described constitution, when the disk medium 100 is mounted on the tray 106 as shown in figure 3(a), the tray 106 is housed into the recording and reproduction apparatus 200,

the disk medium 100 is clamped down from above and beneath by the clipping 107 and the spindle motor 109 and is rotated by the spindle motor 109, the data area 102 of the disk medium 100 is accessed by the optical pickup 208, and data to be recorded/reproduced are communicated to an after-mentioned cipher part. When the clipping 107 fixes the disk medium 100, the wiring arranged on the disk medium 100 comes in contact therewith, whereby the recording and reproduction apparatus 200 and the semiconductor tip 101 embedded in the disk medium 100 can perform data communication through the data lines.

Page 27, first full paragraph, cancel and replace with:

In Step A203, the CPU 203 transfers the title and the-number-of-digital-output-restriction-times information to the medium management part 202 based on the information set in the user setting part 206, and a random number is generated from the random number part 211 to create an encryption key (key A). In Step A204, the program A as analog data is inputted to the A/D converter 209, where it is converted into digital data, is further transmitted to the signal processing part 201, where the program A is made into a

record format, is transmitted to the cipher part 210, where the program A is encrypted employing the key A, and is transmitted to the optical pickup 208, and the encrypted program A is recorded in a vacant area of the data area 102 on the disk medium 100 and a title of the recorded data and arrangement of data in the disk medium 100 are recorded in the TOB area 104 from the optical pickup 208 by a control of the CPU 203.

Page 28, fourth full paragraph, cancel and replace with:

In this way, writing of a content onto the disk medium 100 is performed.

Page 29, second full paragraph, cancel and replace with:

In Step A403, the CPU 203 transmits a start command indicating reproduction start, the title to be reproduced, and the information of presence or absence of digital output from the medium management part 202 to the semiconductor tip 101 through the data lines.

Page 30, third full paragraph to Page 31, paragraph continued, cancel and replace with:

Here, the set information in Step A402 cannot be modified after the end of Step A403, and thus the set information is erased and setting is reattempted from Step A402 in case of modification. Therefore, even when digital output is set to "absence" in Step A402 and is modified to "presence" after the end of Step A402, unjustified digital output of a content which cannot be digitally outputted can be prevented by StepA407.

Page 49, first paragraph, cancel and replace with:

Figure 36 is a block diagram illustrating a constitution of a semiconductor tip 101d in the fifth embodiment, in which numeral 119 denotes a cipher part of a recoding and reproduction apparatus 400 in the fifth embodiment shown in figure 37, which has the same cipher algorithm as that of the cipher part 210, numeral 120 denotes a random number part which generates a random number, and numeral 121 denotes a key box part as a set of key arrangement employed in the cipher part 119. Other parts are the same as those

shown in figure 4, and their descriptions will be omitted here. Figure 37 is a block diagram of a recording and reproduction apparatus 400 in the fifth embodiment, in which numeral 214 denotes a key box part having the same function as that of the key box part 121 included in the semiconductor tip 101d mounted on the disk medium 100. The same reference numerals as those shown in figure 5 denote the same or corresponding parts.

Page 53, third full paragraph, cancel and replace with:

While in the first embodiment, the semiconductor tip 101 which the pins 133 is connected to is embedded in the base material layer 131 with a concave portion and both sides thereof are applied with the recording layers 132, thereby to manufacture the disk medium 100, it is also possible that only a part of the clipping area 103 having the semiconductor tip 101 and the wiring 105 is created separately and is embedded in the disk medium 100, which has the outside of the clipping area 103 created conventionally.

Page 54, second paragraph, cancel and replace with:

Further, while a password is held in the disk medium 100 as personal information so as to be confirmed in the third embodiment, or a cipher processing is employed to perform authentication between the disk medium 100 and the recording and reproduction apparatus 400 in the fifth embodiment, it is also possible that an algorithm for authentication is held in a medium such as an IC card, which is employed instead of a key at content reproduction, thereby to prevent unjustified use.

IN THE CLAIMS:

Please amend claims 3, 5, 7, 9, 11, 12 and 14 as follows:

3. (Amended) The data recording medium as defined in Claim 1, wherein

the content is encrypted employing a key and is recorded on the data recording medium, and

the reproduction history management circuit comprises: a storage part for storing a decryption key for decrypting the content recorded on the data recording medium; and

a content output management part for restricting the number of output times of the decrypted content in digital format when a content is reproduced from the data recording medium.

5. (Amended) The data recording medium as defined in Claim 3, wherein

when the content is outputted in digital format, the content output management part updates and records its number of times, compares the number of times with the previously set number of restriction times, and decides not to output the content in digital format when the number of output times of the content in digital format exceeds the number of restriction times.

7. (Amended) The data recording medium as defined in Claim 1, wherein

the content output management part has personal information storage part for storing personal information for authenticating an owner of the data recording medium and compares externally inputted information with the personal information and permits reproduction of the content only when the comparison results in matching, at reproduction of the content.

9. (Amended) The data recording medium as defined in Claim

1, wherein

the content output management part further has a cipher processing part for performing an encryption processing according to a prescribed algorithm and performs authentication by a cipher between the data recording medium and the recording and reproduction apparatus, and suppresses reproduction of the content according to the authentication result.

11. (Amended) The data management system as defined in Claim 10, wherein

the recording and reproduction apparatus has plural digital output openings,

the reproduction history management circuit further records the number of paths when the content is outputted in digital format simultaneously through plural paths, and

the number of paths is added by the reproduction history management circuit to restrict the number of output times, when the content is outputted in digital format through the plural paths.

12. (Amended) The data management system as defined in Claim

10, wherein

the reproduction history management circuit further records personal information for recognizing an owner of the data recording medium, and

when the content is reproduced, externally inputted information is compared with the personal information held by the reproduction history management circuit, and reproduction of the content is suppressed according to the comparison result.

14. (Amended) The data management system as defined in Claim 10, wherein

the reproduction history management circuit subjects a cipher key to an encryption processing according to a prescribed algorithm,

the medium management part subjects the cipher key to an encryption processing by the same algorithm as that of the reproduction history management circuit, and

when the content is reproduced, authentication is performed between the data recording medium and the recording and reproduction apparatus employing the encryption processing by the

reproduction history management circuit and the encryption processing of the medium management part, and whether or not the content can be decrypted is judged according to the authentication result.

REMARKS

Claims 1-14, as amended, remain herein.

This Preliminary Amendment is to conform the application Article 34 amendments to the specification and claims and to eliminate multiply dependent claims from the above-identified application.

Examination of this application on its merits is respectfully requested.

Respectfully submitted,

PARKHURST & WENDEL, L.L.P.

November 30, 2001
Date

Roger W. Parkhurst
Registration No. 25,177

Attachment:
Specification and Claims Mark Up

RWP/ame

Attorney Docket No. HYAE:128

PARKHURST & WENDEL, L.L.P.
1421 Prince Street, Suite 210
Alexandria, Virginia 22314-2805
Telephone: (703) 739-0220

which compares the externally inputted information with the personal information and stores the number of mismatch times when the comparison successively results in mismatch, and suppresses reproduction of the content as well as informs the outside of the mismatch when the number of mismatch times exceeds a prescribed value.

According to the so-constituted data recording medium, the content output management part has the-number-of-mismatch-times holding part and stores the number of mismatch times as a result of comparing externally inputted information with personal information and suppresses output of a content as well as inform the outside of the mismatch when the number of mismatch times exceeds a prescribed value, thereby preventing unspecified people other than an owner of the data recording medium from reproducing the content without authorization.

According to Claim 9 of the present invention, in the data ~~storing~~ recording medium as defined in any of Claims 1 to 8, the content output management part further has a cipher processing part for performing an encryption processing according to a prescribed algorithm and performs authentication by a cipher between the data recording medium and the recording and reproduction apparatus, and suppresses reproduction of the content according to the authentication result.

According to the so-constituted data recording medium, the cipher processing part is provided in the reproduction history

According to Claim 11 of the present invention, in the data management system as defined in Claim 10, the recording and reproduction apparatus has plural digital output openings, the reproduction history management circuit further records the number of paths when the content is outputted in digital format simultaneously through plural paths, and the number of paths is added by the reproduction history management circuit to restrict the number of output times, when the content is outputted in digital format through the plural paths.

~~In~~ According to the so-constituted data management system, in a recording and reproduction apparatus having plural digital output openings, the reproduction history management circuit records the number of plural paths and adds the number of paths to the number of output times in digital format output for restriction thereof, whereby the number of copy times can be restricted when a reproduced content is digitally copied simultaneously employing plural digital outputs.

According to Claim 12 of the present invention, in the data management system as defined in Claim 10 or 11, the reproduction history management circuit further records personal information for recognizing an owner of the data recording medium, and when the content is reproduced, externally inputted information is compared with the personal information held by the reproduction history management circuit, and reproduction of the content is suppressed according to the

comparison result.

According to the so-constituted data management system, personal information held by the reproduction history management circuit and externally inputted information are compared and reproduction of a content is suppressed according to its result, whereby an unjustified copy by one other than an owner of this content can be prevented, resulting in enhancement in content security.

According to Claim 13 of the present invention, in the data management system as defined in Claim 12, the reproduction history management circuit further records the number of mismatch times of a result of the comparison, and when the content is reproduced, a previously set number of times is compared with the number of mismatch times held by the reproduction history management circuit, thereby to suppress reproduction of the content.

~~In~~ According to the so-constituted data management system, the number of mismatch times held by the reproduction history management circuit is compared with a prescribed value and reproduction of a content is suppressed, whereby it is possible to warn an owner of the content of an unjustified access by one other than the owner, resulting in further enhancement in content security.

According to Claim 14 of the present invention, in the data management system as defined in any of Claims 10 to 13,

Step Z3 at recording of the data management system according to the first embodiment.

Figure 10 is a diagram for explaining an overall operation when the content recorded on the disk medium according to the first embodiment is reproduced by the recording and reproduction apparatus.

Figure 11 is a diagram illustrating a detailed process of Step ~~A2~~ A1 when the content of the data management system according to the first embodiment is reproduced.

Figure 12 is a diagram illustrating a detailed process of Step A2 when the content of the data management system according to the first embodiment is reproduced.

Figure 13 is a diagram illustrating a detailed process of Step A3 when the content of the data management system according to the first embodiment is reproduced.

Figure 14 is a diagram illustrating a detailed process of Step A4 when the content of the data management system according to the first embodiment is reproduced.

Figure 15 is a block diagram schematically illustrating a constitution of a semiconductor tip mounted on a disk medium as a data recording medium according to a second embodiment.

Figure 16 is a block diagram illustrating an overall constitution of a data management system employing the data recording medium according to the second embodiment.

Figure 17 is a diagram for explaining an overall operation

Figure 25 is a diagram illustrating a detailed process of Step C2 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 26 is a diagram illustrating a detailed process of Step C3 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 27 is a diagram illustrating a detailed process of Step C4 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 28 is an overall block diagram illustrating a procedure for confirming registered personal information of the data management system employing the data recording medium according to the third embodiment.

Figure 29 is a diagram illustrating a detailed process of Step D3 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

Figure 30 is a diagram illustrating a detailed process of Step ~~D4~~ D5 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

Figure 31 is a diagram illustrating a detailed process of Step D4 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

(Embodiment 1)

Figure 1 is a diagram illustrating a conceptual constitution of a disk medium 100 as a data recording medium according to a first embodiment of the present invention. In figure 1, numeral 90 denotes a center hole, numeral 100 denotes a disk medium such as a DVD-RAM composed of polycarbon, numeral 101 denotes a semiconductor tip (reproduction history management circuit) which includes a nonvolatile semiconductor tip or the like as a storage element, numeral 102 denotes a data area, numeral 103 denotes a clipping area for fixing the disk medium 100 on an after-mentioned rotation drive, and numeral 104 denotes a TOB (Table of contents) area where management information of the ~~recorded~~ data area 102 on the disk medium 100 is recorded.

When there may be plural semiconductor tips, for example, when there are two semiconductor tips, they may be arranged to be symmetrized with the center hole 90 in the center, thereby to achieve a balance, while there is one here.

Figure 2 is a diagram exemplifying arrangement of wires provided in the disk medium for performing electrical signal connection with the semiconductor tip 101 mounted on the disk medium 100. In the figure, numeral 105 denotes wiring provided in the clipping area 103, which comprises a data line as a two-way signal line, a power line for supplying power, a clock line for supplying a clock when the semiconductor tip 101 is driven,

reading a pit formed in the data area 102 of the disk medium 100.

The constitution of the disk medium 100 in more detail is as follows; the disk medium 100 comprises three layers as shown in figure 3(c), in which numeral 131 denotes a base material layer and numeral 132 denotes a recording layer in which contents are recorded. In the semiconductor tip 101, pins 133 corresponding to the respective wiring 105 provided in the clipping area 103 are attached, by which the semiconductor tip 101 and the wiring 105 are connected so that power, a signal and the like are supplied to the semiconductor tip 101 as described above.

Its manufacturing method is as follows; the semiconductor tip ~~105~~101 to which the pins 133 are attached is embedded in the base material layer 131 having a concave portion in a part of the clipping area 103. Then, the recording layers 132 are applied to both sides and the wiring 105 corresponding to respective pins 133 is formed in a metal pattern on the surface from which the pins 133 are protruding by masking or the like. While the disk medium 100 comprises three layers here, it may also comprise two layers with the recording medium layer on only one side.

With the above-described constitution, when the disk medium 100 is mounted on the tray 106 as shown in figure 3(a), the tray 106 is housed into the recording and reproduction

apparatus 200, the disk medium 100 is clamped down from above and beneath by the clipping 107 and the spindle motor 109 and is rotated by the spindle motor 109, the data area 102 of the disk medium 100 is accessed by the optical pickup 208, and data to be recorded/reproduced are communicated to an after-mentioned cipher part. When the clipping 107 fixes the disk medium 100, the wiring arranged on the disk medium 100 comes in contact therewith, whereby the recording and reproduction apparatus 200 and the semiconductor tip 101 embedded in the disk medium 100 can perform data communication through the data lines.

Next, an operation will be described.

First, a recording operation will be described with reference to figures 4 to 9.

When a content is encrypted to be recorded onto the disk medium 100, the semiconductor tip 101 has an I/O 100 as a two-way communication port, a CPU 111 (content output management part) which controls a data signal and a control signal and performs arithmetic operations, and a storage part 112 composed of a nonvolatile memory such as an EPROM and an EEPROM, which holds management information of recorded data, as shown in figure 4.

Table 1 shows contents of the information held in the storage part 112, in which numeral 114 denotes a title, numeral 115 denotes a decryption key part holding a decryption key in

the like on the disk medium 100, by the optical pickup 208 accessing the TOB area 104 on the disk media 104, and displays the title on the display part 207.

Next, in Step A202, a title of content data to be recorded by a user, the-number-of-digital-output-restriction-times information, presence or absence of encryption of the content are set into the user setting part 206 (here, title: program A, the-number-of-digital-output-restriction-times information: 5, and encryption: presence).

In Step A203, the CPU 203 transfers the title and the-number-of-digital-output-restriction-times information to the medium management part 202 based on the information set in the user setting part 206, and a random number is generated from the random number part 211 to create an encryption key (key A). In Step A204, the program A as analog data is inputted to the A/D converter 209, where it is converted into digital data, is further transmitted to the signal processing part 201, where the program A is made into a record format, is transmitted to the cipher part 210, where the program A is encrypted employing the key A, and is transmitted to the optical pickup 208, and the encrypted program A is recorded in a vacant area of the ~~recording~~ data area 102 on the disk medium 100 and a title of the recorded data and arrangement of data in the disk medium 100 are recorded in the TOB area 104 from the optical pickup 208 by a control of the CPU 203.

In Step A205, the medium management part 202 transmits a registration command, the title (program A), the-number-of-digital-output-restriction-times information (5), and the key A to the semiconductor tip 101 through the data lines.

In figure 8 as a process in Step Z2, in Step A208, the registration command, the title (program A), the-number-of-digital-output-restriction-times information (5), and the key A are received by the I/O 110.

In Step A209, by the registration command received by the I/O 110, the CPU 111 transmits the received information in Step A208 to the storage part 112, where the information is stored as shown in Table 1.

In Step A210, an end of communication is transmitted to the medium management part 202 after recording.

In figure 9 as a process in Step Z3, the end of communication is received in step A213 and the operation for recording setting information onto the disk medium is ended.

In this way, writing of a content onto the disk medium 100 is performed.

Next, an operation for reproducing the disk medium 100 on which a content is recorded being encrypted in the recording and reproduction apparatus 200 will be described with reference to figures 10 to 14.

As shown in figure 10, Steps A1 and A3 are performed in the recording and reproduction apparatus 200 and Steps A2 and

A4 are performed in the semiconductor tip 101, and they are performed in the order of Steps A1-A4.

First, in figure 11 as a process in Step A1, in Step A401, when the disk medium 100 is arranged in the recording and reproduction apparatus 200 as shown in figure 3, the CPU 203 detects a title and arrangement of data recorded by a user, a vacant area, and the like on the disk medium 100, by the optical pickup 208 accessing the TOB area 104 on the disk media 100, and displays the title on the display part 207.

Next, in Step A402, presence or absence of output of a title to be reproduced by a user from the digital interface 204 to the external recording and reproduction apparatus 212 through the connection cable 213 is set into the CPU 203 through the user setting part 206 (title: program A, digital output: presence).

In Step A403, the CPU 203 transmits a start command indicating reproduction start, the title to be reproduced, and the information of presence or absence of digital output from the medium management part 202 to the semiconductor tip 101 through the data lines ~~108 and 105~~.

In figure 12 as a process in Step A2, the semiconductor tip 101 receives the information set in Step A402 at the I/O 110 and the CPU 111 confirms the start command in Step A406, and presence or absence of digital output is confirmed in Step A407. When there is no digital output (no), the processing

A402 is prompted visually or aurally in the display part 207.

Here, the set information in Step A402 cannot be modified after the end of Step A403, and thus the set information is erased and setting is reattempted from Step A402 in case of modification. Therefore, even when digital output is set to "absence" in Step A402 and is modified to "presence" after the end of Step A402, unjustified digital output of a content which cannot be digitally outputted can be prevented by Step ~~A408~~A407.

On the other hand, in case of no reproduction non-permission command (no) in Step A415, the processing proceeds to Step A417, where presence or absence of digital output set in Step A402 is confirmed, and in case of "presence" (yes), the processing proceeds to Step A418, where a content of the title (program A) set in Step A402 is reproduced employing the decryption key (key A) received in Step A414 and decrypted data are outputted from the digital interface 204 in digital format, and a reproduction end is transmitted to the semiconductor tip 101 when the reproduction is ended in Step A419.

In Step A417, when presence of absence of digital output set in Step A402 is confirmed and it is "absence" (no), the processing proceeds to Step S420, where the content of the title (program A) set in Step A402 is decrypted employing the decryption key (key A) received in Step S414 and is reproduced in analog format from the D/A converter 205.

In figure 14 as a process in Step A4, when the

be described. In the fifth embodiment, an authenticating operation employing a cipher is performed in the above-described respective embodiments. Here, a description will be given exemplifying a case where this embodiment is applied in the first embodiment.

Figure 36 is a block diagram illustrating a constitution of a semiconductor tip 101d in the fifth embodiment, in which numeral 119 denotes a cipher part of ~~the~~ a recoding and reproduction apparatus ~~200~~ 400 in the fifth embodiment shown in figure 37, which has the same cipher algorithm as that of the cipher part 210, numeral 120 denotes a random number part which generates a random number, and numeral 121 denotes a key box part as a set of key arrangement employed in the cipher part 119. Other parts are the same as those shown in figure 4, and their descriptions will be omitted here. Figure 37 is a block diagram of a recording and reproduction apparatus 400 in the fifth embodiment, in which numeral 214 denotes a key box part having the same function as that of the key box part 121 included in the semiconductor tip 101d mounted on the disk medium 100. The same reference numerals as those shown in figure 5 denote the same or corresponding parts.

Table 2 shows information held in the key box part 121 and the key box part 214, in which numeral 1700 denotes a key code for selecting a key and numeral 1701 denotes a key selected according to the key code 1700.

G1826.

In figure 43 as a process in Step G5, the continuation command or the transmission end is received in Step G1531, it is confirmed whether the received information is a continuation command or not in Step G1532, and in case where this is judged not to be a continuation command (no), the processing proceeds to Step G1534, where communication is ended, while in case where this is judged to be a continuation command, the processing proceeds to Step G1533, where a reproduction operation is performed.

As described above, according to the fifth embodiment, a cipher processing function is provided with the semiconductor tip 101d of the disk medium 100 and authentication is performed employing a cipher, whereby reproduction of the disk medium 100 is permitted only in the environment enabling cipher communication, resulting in further enhancement in content security.

Further, a transmission key for encrypting and transmitting data required for a recording or reproduction operation is generated differently for each authentication, employing data in communication process including random number data, whereby a high-security key can be created.

While in the first embodiment, the semiconductor tip 101 which the pins 133 is connected to is embedded in the base material ~~part~~ layer 131 with a concave portion and both sides

thereof are applied with the recording layers 132, thereby to manufacture the disk medium 100, it is also possible that only a part of the clipping area 103 having the semiconductor tip 101 and the wiring 105 is created separately and is embedded in the disk medium 100, which has the outside of the clipping area 103 created conventionally.

Further, while in the first embodiment, the wiring 105 is employed in the clipping area 103 so as to supply power or a signal to the semiconductor tip 101 mounted on the disk medium 100, it is also possible that a solar battery panel is mounted on the clipping area 103 to supply power to the semiconductor tip 101 as well as to irradiate a semiconductor laser to a specified position of the solar battery panel, thereby transferring a signal.

Further, while a password is held in the disk medium 100 as personal information so as to be confirmed in the third embodiment, or a cipher processing is employed to perform authentication between the disk medium 100 and the recording and reproduction apparatus 400 in the fifth embodiment, it is also possible that an algorithm for authentication is held in a medium such as an IC card, which is employed instead of a key at content reproduction, thereby to prevent unjustified use.

APPLICABILITY IN INDUSTRY

As described above, a data recording medium and data

CLAIMS

1. A data recording medium for content recording or reproduction including:

a reproduction history management circuit which records copyright protection information and manages reproduction and output of a content referring to the copyright protection information at content reproduction.

2. The data recording medium as defined in Claim 1,

the data recording medium is made of a recording layer for recording a content and a base material layer, wherein

the reproduction history management circuit is embedded in a part of the base material layer in a clipping area in the data recording medium, and

the clipping area is an area where the data recording medium is fixed with respect to a rotation drive for rotating the data recording medium.

3. The data recording medium as defined in Claim 1~~ or 2~~, wherein

the content is encrypted employing a key and is recorded on the data recording medium, and

the reproduction history management circuit comprises: a

storage part for storing a decryption key for decrypting the content recorded on the data recording medium; and

a content output management part for restricting the number of output times of the decrypted content in digital format when a content is reproduced from the data recording medium.

4. The data recording medium as defined in Claim 3, wherein

the content recorded on the data recording medium is encrypted employing a key different in unit of the title or the arbitrary data size, and

the content output management part has a decryption key for each unit of content encryption and restricts the number of output times of the content in digital format in unit of the title or the arbitrary data size.

5. The data recording medium as defined in Claim 3~~ or 4~~, wherein

when the content is outputted in digital format, the content output management part updates and records its number of times, compares the number of times with the previously set number of restriction times, and decides not to output the content in digital format when the number of output times of the content in digital format exceeds the number of restriction times.

6. The data recording medium as defined in Claim 5, wherein

when the content is outputted in digital format simultaneously through plural paths, the content output management part has an output path number storage part for storing the number of paths, and adds the number of paths stored in the output path number storage part to count outputs of the content in digital format, when the number of output times of the content in digital format is counted.

7. The data recording medium as defined in ~~any of Claims 1 to 6~~ Claim 1, wherein

the content output management part has personal information storage part for storing personal information for authenticating an owner of the data recording medium and compares externally inputted information with the personal information and permits reproduction of the content only when the comparison results in matching, at reproduction of the content.

8. The data recording medium as defined Claim 7, wherein

the content output management part has the-number-of-mismatch-times holding part which compares the externally inputted information with the personal information and stores the number of mismatch times when the comparison successively

results in mismatch, and suppresses reproduction of the content as well as informs the outside of the mismatch when the number of mismatch times exceeds a prescribed value.

9. The data recording medium as defined in ~~any of Claims 1 to 8~~ Claim 1, wherein

the content output management part further has a cipher processing part for performing an encryption processing according to a prescribed algorithm and performs authentication by a cipher between the data recording medium and the recording and reproduction apparatus, and suppresses reproduction of the content according to the authentication result.

10. A data management system for managing data employing a data recording medium for content recording or reproduction, wherein

the data recording medium has a reproduction history management circuit which records copyright protection information and manages reproduction and output of a content referring to the copyright protection information at content reproduction,

the recording and reproduction apparatus has a medium management part which is connected to the reproduction history management circuit and manages writing or reading of data on the data recording medium, and

when the content is reproduced, an encrypted content is decrypted by a decryption key held in the reproduction history management circuit to be reproduced, and when it is outputted in digital format, the number of output times is restricted by the reproduction history management circuit.

11. The data management system as defined in Claim 10, wherein

the recording and reproduction apparatus has plural digital output openings,

the reproduction history management circuit further records the number of paths when the content is outputted in digital format simultaneously through plural paths, and

the number of paths is added by the reproduction history management circuit to restrict the number of output times, when the content is outputted in digital format through the plural paths.

12. The data management system as defined in Claim 10~~ or 11~~, wherein

the reproduction history management circuit further records personal information for recognizing an owner of the data recording medium, and

when the content is reproduced, externally inputted information is compared with the personal information held by the reproduction history management circuit, and reproduction

of the content is suppressed according to the comparison result.

13. The data management system as defined in Claim 12, wherein

the reproduction history management circuit further records the number of mismatch times of a result of the comparison, and

when the content is reproduced, a previously set number of times is compared with the number of mismatch times held by the reproduction history management circuit, thereby to suppress reproduction of the content.

14. The data management system as defined in ~~any of Claims 10 to 13~~ Claim 10, wherein

the reproduction history management circuit subjects a cipher key to an encryption processing according to a prescribed algorithm,

the medium management part subjects the cipher key to an encryption processing by the same algorithm as that of the reproduction history management circuit, and

when the content is reproduced, authentication is performed between the data recording medium and the recording and reproduction apparatus employing the encryption processing by the reproduction history management circuit and the encryption processing of the medium management part, and whether or not the content can be decrypted is judged according

to the authentication result.

DESCRIPTION

DATA RECORDING MEDIUM AND DATA MANAGEMENT SYSTEM

TECHNICAL FIELD

The present invention relates to a data recording medium and a data management system and, more particularly, to an art for improving copyright protection of a content for digital copy.

BACKGROUND ART

While digitalization of contents is making progress, copyright protection by a digital copy has become a problem since a digital copy has no deterioration. Therefore, there is proposed CGMS (Copy Generation Management System) method which indicates copyright protection information by four states of Free, Never Copy, One More Copy, and No More Copy as shown in figure 44. Figure 45 illustrates a reproduction apparatus 504 which is provided with digital output that controls copyright protection by the CGMS method. In figure 45, numeral 500 denotes a disk medium such as a CD-ROM and numeral 504 denotes a reproduction apparatus. The reproduction apparatus 504 comprises a reproduction signal processing circuit 501 for processing a signal read from the disk medium employing an optical pickup 506 or the like, a digital interface 503 for

outputting a reproduction signal, and a CPU 502 for controlling operations of the reproduction signal processing circuit 501 and digital interface 503.

Hereinafter, a description will be given of a control of digital output of a content employing the CGMS method in the conventional reproduction apparatus 504 which is provided with digital output that controls copyright protection.

First, CGMS information added to the disk medium 500 is transferred from the reproduction signal processing circuit 501 to the CPU 502. The CPU 502 controls digital output of reproduction data of the disk medium 500 from the digital interface 503 according to the CGMS information as follows.

1. When the CGMS is "Free", output of the reproduction data from the digital interface 503 is always admitted.

2. When the CGMS is "Never Copy", output of the reproduction data from the digital interface 503 is not admitted.

3. When the CGMS is "One More Copy", output of the reproduction data from the digital interface 503 is admitted only once.

4. When the CGMS is "No More Copy", output of the reproduction data from the digital interface 503 is not admitted.

Here, in a case where a recording apparatus is connected to the digital interface 503 and data of "One More Copy" are

outputted to the recording apparatus, the information of "One More Copy" is rewritten to that of "No More Copy" on the side of the recording apparatus and data are recorded and managed onto the recording medium anew.

Further, in view of the fact that a copy from an original disk medium is infinitely possible when the CGMS information of a content is "One More Copy" in the above-described constitution, there may be also a method in which a management information area 505 where information for controlling the number of copy times can be recorded on the surface of the disk medium 500 is provided, the reproduction apparatus is constituted so as to prohibit copying when the information reached a prescribed value, the number of copy times is rewritten every time a content of "One More Copy" is copied, and a subsequent copy from the original disk medium is suppressed when the number of copy times matches the prescribed value.

Further, Japanese Published Patent Application No. Hei. 7-161172 discloses a data recording medium in which recording can be performed with high-security and user-friendliness when various data are recorded onto a recording medium such as a disk and a tape. This data recording medium is constituted such that a recording medium on which data are recorded is stored in a chassis and an IC is attached to a prescribed point of the chassis. A startup program and encrypted data are

recorded on the recording medium, a encryption program and password data of the recorded data are stored in a memory in the IC, and when the recorded data are read or data are written into the recording medium, an inputted password is supplied to the IC to be collated with the password stored in the memory in the IC by an arithmetic operation means, and encrypted data stored in the recording medium are decrypted or data to be recorded onto the recording medium are encrypted according to the encryption program stored in the memory in the IC when the passwords match, thereby enabling high-security and user-friendly recording with no complicated keyword management by the IC including an encrypted program, which is provided in the chassis.

Though a content duplicated from a conventional recording medium having the CGMS information is subjected to rewriting of its CGMS information at recording onto a recording medium so that the content is not further duplicated, the number of digital copy times onto the recording medium can not be restricted when the CGMS information is "One More Copy" in the above-described conventional constitution, whereby it is impossible to effectively prevent copyright piracy by a digital copy of a content.

Further, even when a rewritable area for managing the number of copy times is provided in a prescribed area of a disk medium, it is impossible to effectively prevent copyright

piracy by a so-called stamp copy, by which a pit shape formed on the disk medium is physically copied.

Further, in the data recording medium disclosed in the Japanese Published Patent Application No. Hei. 7-161172, an encryption program of an encrypted content recorded on the data recording medium is held in the IC which is attached to the chassis storing the data recording medium, whereby the data recording medium may be copied by employing the encryption program in the IC, that is, the chassis attached with the IC and the data recording medium body are separated to be employed for a illegal copy.

The present invention is made to solve the above-mentioned conventional problems and has for its object to provide high-security copyright management in a disk medium.

DISCLOSURE OF THE INVENTION

According to Claim 1 of the present invention, a data recording medium for content recording or reproduction including: a reproduction history management circuit which records copyright protection information and manages reproduction and output of a content referring to the copyright protection information at content reproduction.

According to the so-constituted data recording medium, the reproduction history management circuit is provided in the data recording medium, thereby managing reproduction of a content on

its own and preventing unrestricted duplication employing a recording medium as a copy source, resulting in effective prevention of copy right piracy.

According to Claim 2 of the present invention, the data recording medium as defined in Claim 1 is made of a recording layer for recording a content and a base material layer, the reproduction history management circuit is embedded in a part of the base material layer in a clipping area in the data recording medium, and the clipping area is an area where the data recording medium is fixed with respect to a rotation drive for rotating the data recording medium.

According to the so-constituted data recording medium, the reproduction history management circuit is embedded in the base material part of the data recording medium, whereby an encryption program, which is embedded, is not copied even when a physical stamp copy is performed, and a content is destroyed when it is to be taken out, resulting in higher-security copyright management.

According to Claim 3 of the present invention, in the data recording medium as defined in Claim 1 or 2, the content is encrypted employing a key and is recorded on the data recording medium, and the reproduction history management circuit comprises: a storage part for storing a decryption key for decrypting the content recorded on the data recording medium; and a content output management part for restricting the number

of output times of the decrypted content in digital format when a content is reproduced from the data recording medium.

According to the so-constituted data recording medium, a content is encrypted and recorded on the data recording medium, a decryption key for decrypting the content is held in the reproduction history management circuit, and the number of output times is restricted in digital format, whereby the content, which is encrypted, is not reproduced even when a physical stamp copy is performed, and copying for more than a prescribed number of times is impossible since the number of output times is restricted in case of reproduction, resulting in effective prevention of copyright piracy.

According to Claim 4 of the present invention, in the data recording medium as defined in Claim 3, the content recorded on the data recording medium is encrypted employing a key different in unit of the title or the arbitrary data size, and the content output management part has a decryption key for each unit of content encryption and restricts the number of output times of the content in digital format in unit of the title or the arbitrary data size.

According to the so-constituted data recording medium, encryption is performed employing a key different in unit of the title or arbitrary data size of a content, and the number of output times in digital format is restricted in unit of the title or the arbitrary data size, resulting in firm copyright

of the content.

According to Claim 5 of the present invention, in the data recording medium as defined in Claim 3 or 4, when the content is outputted in digital format, the content output management part updates and records its number of times, compares the number of times with the previously set number of restriction times, and decides not to output the content in digital format when the number of output times of the content in digital format exceeds the number of restriction times.

According to the so-constituted data recording medium, the content output management part updates the number of digital output times and records the updated number of times, compares it with the previously set number of restriction times, and decides not to perform digital output according to its result, whereby the number of content duplication times in digital format can be restricted.

According to Claim 6 of the present invention, in the data recording medium as defined in Claim 5, when the content is outputted in digital format simultaneously through plural paths, the content output management part has an output path number storage part for storing the number of paths, and adds the number of paths stored in the output path number storage part to count outputs of the content in digital format, when the number of output times of the content in digital format is counted.

According to the so-constituted data recording medium, when a content is outputted in digital format simultaneously through plural paths, the output path number storage part adds the number of paths for counting, whereby the number of duplication times can be restricted even in a reproduction apparatus provided with plural output interfaces in digital format.

According to Claim 7 of the present invention, in the data recording medium as defined in any of Claims 1 to 6, the content output management part has personal information storage part for storing personal information for authenticating an owner of the data recording medium and compares externally inputted information with the personal information and permits reproduction of the content only when the comparison results in matching, at reproduction of the content.

According to the so-constituted data recording medium, the content output management part has the personal information storage part and compares externally inputted information with personal information and permits reproduction only in case of their matching at content reproduction, thereby preventing unspecified people other than an owner of the data recording medium from reproducing the content without authorization.

According to Claim 8 of the present invention, in the data recording medium as defined Claim 7, the content output management part has the-number-of-mismatch-times holding part

which compares the externally inputted information with the personal information and stores the number of mismatch times when the comparison successively results in mismatch, and suppresses reproduction of the content as well as informs the outside of the mismatch when the number of mismatch times exceeds a prescribed value.

According to the so-constituted data recording medium, the content output management part has the-number-of-mismatch-times holding part and stores the number of mismatch times as a result of comparing externally inputted information with personal information and suppresses output of a content as well as inform the outside of the mismatch when the number of mismatch times exceeds a prescribed value, thereby preventing unspecified people other than an owner of the data recording medium from reproducing the content without authorization.

According to Claim 9 of the present invention, in the data storing medium as defined in any of Claims 1 to 8, the content output management part further has a cipher processing part for performing an encryption processing according to a prescribed algorithm and performs authentication by a cipher between the data recording medium and the recording and reproduction apparatus, and suppresses reproduction of the content according to the authentication result.

According to the so-constituted data recording medium, the cipher processing part is provided in the reproduction history

management circuit and authentication is performed between the reproduction history circuit and the data recording medium, thereby further enhancing security of a content.

According to Claim 10 of the present invention, in a data management system for managing data employing a data recording medium for content recording or reproduction, the data recording medium has a reproduction history management circuit which records copyright protection information and manages reproduction and output of a content referring to the copyright protection information at content reproduction, the recording and reproduction apparatus has a medium management part which is connected to the reproduction history management circuit and manages writing or reading of data on the data recording medium, and when the content is reproduced, an encrypted content is decrypted by a decryption key held in the reproduction history management circuit to be reproduced, and when it is outputted in digital format, the number of output times is restricted by the reproduction history management circuit.

According to the so-constituted data management system, writing or reading of data on the data recording medium is managed in the medium management part connected to the reproduction history management circuit and output in digital format is restricted by the reproduction history management circuit, thereby providing a system effectively protecting copyright of a content.

According to Claim 11 of the present invention, in the data management system as defined in Claim 10, the recording and reproduction apparatus has plural digital output openings, the reproduction history management circuit further records the number of paths when the content is outputted in digital format simultaneously through plural paths, and the number of paths is added by the reproduction history circuit to restrict the number of output times, when the content is outputted in digital format through the plural paths.

In the so-constituted data management system, in a recording and reproduction apparatus having plural digital output openings, the reproduction history circuit records the number of plural paths and adds the number of paths to the number of output times in digital format output for restriction thereof, whereby the number of copy times can be restricted when a reproduced content is digitally copied simultaneously employing plural digital outputs.

According to Claim 12 of the present invention, in the data management system as defined in Claim 10 or 11, the reproduction history management circuit further records personal information for recognizing an owner of the data recording medium, and when the content is reproduced, externally inputted information is compared with the personal information held by the reproduction history management circuit, and reproduction of the content is suppressed according to the

comparison result.

According to the so-constituted data management system, personal information held by the reproduction history management circuit and externally inputted information are compared and reproduction of a content is suppressed according to its result, whereby an unjustified copy by one other than an owner of this content can be prevented, resulting in enhancement in content security.

According to Claim 13 of the present invention, in the data management system as defined in Claim 12, the reproduction history management circuit further records the number of mismatch times of a result of the comparison, and when the content is reproduced, a previously set number of times is compared with the number of mismatch times held by the reproduction history circuit, thereby to suppress reproduction of the content.

In the so-constituted data management system, the number of mismatch times held by the reproduction history management circuit is compared with a prescribed value and reproduction of a content is suppressed, whereby it is possible to warn an owner of the content of an unjustified access by one other than the owner, resulting in further enhancement in content security.

According to Claim 14 of the present invention, in the data management system as defined in any of Claims 10 to 13, the reproduction history management circuit subjects a cipher

key to an encryption processing according to a prescribed algorithm, the medium management part subjects the cipher key to an encryption processing by the same algorithm as that of the reproduction history management circuit, and when the content is reproduced, authentication is performed between the data recording medium and the recording and reproduction apparatus employing the encryption processing by the reproduction history management circuit and the encryption processing of the medium management part, and whether or not the content can be decrypted is judged according to the authentication result.

According to the so-constituted data management system, an authentication operation employing a cipher is performed between the recording and reproduction apparatus and the data recording medium, whereby reproduction of a content is permitted only in the environment enabling cipher communication, resulting in enhancement in content security.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a diagram illustrating a conceptual constitution of a disk medium as a data recording medium according to a first embodiment.

Figure 2 is diagram illustrating the constitution of the disk medium which includes wiring in the first embodiment.

Figure 3(a) is a diagram illustrating arrangement of a

recording and reproduction apparatus and the disk medium, which are used when a content recorded on the disk medium in the first embodiment is reproduced or a content is recorded.

Figure 3(b) is a diagram illustrating a state where the disk medium, which is used when the content recorded on the disk medium in the first embodiment is reproduced or a content is recorded, is installed in a motor for rotating it.

Figure 3(c) is a diagram illustrating the constitution of the disk medium in the first embodiment in more detail.

Figure 4 is a block diagram schematically illustrating a constitution of a semiconductor tip in the first embodiment.

Figure 5 is a block diagram illustrating an overall constitution of a data management system employing the data recording medium according to the first embodiment.

Figure 6 is a diagram illustrating an overall operation when a content is encrypted and recorded employing the data management system according to the first embodiment.

Figure 7 is a diagram illustrating a detailed process of Step Z1 at recording of the data management system according to the first embodiment.

Figure 8 is a diagram illustrating a detailed process of Step Z2 at recording of the data management system according to the first embodiment.

Figure 9 is a diagram illustrating a detailed process of Step Z3 at recording of the data management system according to

the first embodiment.

Figure 10 is a diagram for explaining an overall operation when the content recorded on the disk medium according to the first embodiment is reproduced by the recording and reproduction apparatus.

Figure 11 is a diagram illustrating a detailed process of Step A2 when the content of the data management system according to the first embodiment is reproduced.

Figure 13 is a diagram illustrating a detailed process of Step A3 when the content of the data management system according to the first embodiment is reproduced.

Figure 14 is a diagram illustrating a detailed process of Step A4 when the content of the data management system according to the first embodiment is reproduced.

Figure 15 is a block diagram schematically illustrating a constitution of a semiconductor tip mounted on a disk medium as a data recording medium according to a second embodiment.

Figure 16 is a block diagram illustrating an overall constitution of a data management system employing the data recording medium according to the second embodiment.

Figure 17 is a diagram for explaining an overall operation when a content recorded on the disk medium according to the second embodiment is reproduced by a recording and reproduction apparatus.

Figure 18 is a diagram illustrating a detailed process of

Step B1 when a content of the data management system according to the second embodiment is reproduced.

Figure 19 is a diagram illustrating a detailed process of Step B2 when the content of the data management system according to the second embodiment is reproduced.

Figure 20 is a diagram illustrating a detailed process of Step B3 when the content of the data management system according to the second embodiment is reproduced.

Figure 21 is a diagram illustrating a detailed process of Step B4 when the content of the data management system according to the second embodiment is reproduced.

Figure 22 is a block diagram schematically illustrating a constitution of a semiconductor tip mounted on a disk medium as a data recording medium according to a third embodiment.

Figure 23 is an overall block diagram illustrating a procedure of registering personal information of a data management system employing the data recording medium according to the third embodiment.

Figure 24 is a diagram illustrating a detailed process of Step C1 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 25 is a diagram illustrating a detailed process of Step C2 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 26 is a diagram illustrating a detailed process of

Step C3 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 27 is a diagram illustrating a detailed process of Step C4 as a procedure for registering personal information of the data management system according to the third embodiment.

Figure 28 is an overall block diagram illustrating a procedure for confirming registered personal information of the data management system employing the data recording medium according to the third embodiment.

Figure 29 is a diagram illustrating a detailed process of Step D3 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

Figure 30 is a diagram illustrating a detailed process of Step D4 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

Figure 31 is a diagram illustrating a detailed process of Step D4 as a procedure for confirming the registered personal information of the data management system according to the third embodiment.

Figure 32 is a block diagram schematically illustrating a constitution of a semiconductor tip mounted on a disk medium as a data recording medium according to a fourth embodiment.

Figure 33 is an overall block diagram illustrating a

procedure of recording unjustified access at confirmation of personal information of a data management system employing the data recording medium according to the fourth embodiment.

Figure 34 is a diagram illustrating a detailed process of Step E4 as a procedure for recording unjustified access of the data management system according to the fourth embodiment.

Figure 35 is a diagram illustrating a detailed process of Step E5 as a procedure for recording unjustified access of the data management system according to the fourth embodiment.

Figure 36 is a block diagram schematically illustrating a constitution of a semiconductor tip mounted on a disk medium as a data recording medium according to a fifth embodiment.

Figure 37 is a block diagram illustrating an overall constitution of a data management system employing the data recording medium according to the fifth embodiment.

Figure 38 is a diagram for explaining an overall operation when authentication by a cipher algorithm when a content of the data management system according to the fifth embodiment is reproduced is performed.

Figure 39 is a diagram illustrating a detailed process of Step G1 as a procedure for performing authentication of the data management system according to the fifth embodiment.

Figure 40 is a diagram illustrating a detailed process of Step G2 as a procedure for performing authentication of the data management system according to the fifth embodiment.

Figure 41 is a diagram illustrating a detailed process of Step G3 as a procedure for performing authentication of the data management system according to the fifth embodiment.

Figure 42 is a diagram illustrating a detailed process of Step G4 as a procedure for performing authentication of the data management system according to the fifth embodiment.

Figure 43 is a diagram illustrating a detailed process of Step G5 as a procedure for performing authentication of the data management system according to the fifth embodiment.

Figure 44 is a diagram for explaining CGMS (Copy Generation Management System) method as an example of a copyright protection method according to a conventional data management system.

Figure 45 is a block diagram illustrating an overall constitution of a conventional data management system employing a data recording medium.

BEST MODE TO EXECUTE THE INVENTION

Hereinafter, a data recording medium and data management system according to the present invention will be described with reference to figures.

(Embodiment 1)

Figure 1 is a diagram illustrating a conceptual constitution of a disk medium 100 as a data recording medium according to a first embodiment of the present invention. In

figure 1, numeral 90 denotes a center hole, numeral 100 denotes a disk medium such as a DVD-RAM composed of polycarbon, numeral 101 denotes a semiconductor tip (reproduction history management circuit) which includes a nonvolatile semiconductor tip or the like as a storage element, numeral 102 denotes a data area, numeral 103 denotes a clipping area for fixing the disk medium 100 on an after-mentioned rotation drive, and numeral 104 denotes a TOB (Table of contents) area where management information of the recorded data 102 on the disk medium 100 is recorded.

When there may be plural semiconductor tips, for example, when there are two semiconductor tips, they may be arranged to be symmetrized with the center hole 90 in the center, thereby to achieve a balance, while there is one here.

Figure 2 is a diagram exemplifying arrangement of wires provided in the disk medium for performing electrical signal connection with the semiconductor tip 101 mounted on the disk medium 100. In the figure, numeral 105 denotes wiring provided in the clipping area 103, which comprises a data line as a two-way signal line, a power line for supplying power, a clock line for supplying a clock when the semiconductor tip 101 is driven, and a GND line for supplying ground potential, from the outer circumference of the disk media 100, being arranged circularly in this order.

While wiring is arranged on the surface of only one side

of the disk medium 100 in figure 2, it may be also arranged on both sides.

Figures 3(a) and (b) are a partial top view and a cross sectional view when connection between a recording and reproduction apparatus 200 for performing recording/reproduction employing the disk medium 100 with the above-described constitution and the wiring 105 provided on the disk medium 100 is performed, and figure 3(c) is a cross sectional view illustrating the constitution of the disk medium 100 in more detailed. In figures 3(a) and (b), numeral 106 denotes a tray in which the disk medium 100 is arranged, numeral 107 denotes a clipping for fixing the disk medium 100, and numeral 108 denotes wiring provided on the contact face of the clipping 107 with the disk medium 100 and corresponding to the wiring 105 of the disk medium 100. That is, the wiring 108 comprises a data line, a power line, a clock line, and a GND line, from the outer circumference of the disk media 100, being arranged on a concentric circle. The data line of the wiring 108 is connected to an after-mentioned medium management part.

Numeral 109 denotes a spindle motor for rotating the disk medium 100 and numeral 208 denotes an optical pickup for reading a pit formed in the data area 102 of the disk medium 100.

The constitution of the disk medium 100 in more detail is as follows; the disk medium 100 comprises three layers, in

which numeral 131 denotes a base material layer and numeral 132 denotes a recording layer in which contents are recorded. In the semiconductor tip 101, pins 133 corresponding to the respective wiring 105 provided in the clipping area 103 are attached, by which the semiconductor tip 101 and the wiring 105 are connected so that power, a signal and the like are supplied to the semiconductor tip 101 as described above.

Its manufacturing method is as follows; the semiconductor tip 105 to which the pins 133 are attached is embedded in the base material layer 131 having a concave portion in a part of the clipping area 103. Then, the recording layers 132 are applied to both sides and the wiring 105 corresponding to respective pins 133 is formed in a metal pattern on the surface from which the pins 133 are protruding by masking or the like. While the disk medium 100 comprises three layers here, it may also comprise two layers with the recording medium layer on only one side.

With the above-described constitution, when the disk medium 100 is mounted on the tray 106, the tray 106 is housed into the recording and reproduction apparatus 200, the disk medium 100 is clamped down from above and beneath by the clipping 107 and the spindle motor 109 and is rotated by the spindle motor 109, the data area 102 of the disk medium 100 is accessed by the optical pickup 208, and data to be recorded/reproduced are communicated to an after-mentioned

cipher part. When the clipping 107 fixes the disk medium 100, the wiring arranged on the disk medium 100 comes in contact therewith, whereby the recording and reproduction apparatus 200 and the semiconductor tip 101 embedded in the disk medium 100 can perform data communication through the data lines.

Next, an operation will be described.

First, a recording operation will be described with reference to figures 4 to 9.

When a content is encrypted to be recorded onto the disk medium 100, the semiconductor tip 101 has an I/O 100 as a two-way communication port, a CPU 111 (content output management part) which controls a data signal and a control signal and performs arithmetic operations, and a storage part 112 composed of a nonvolatile memory such as an EPROM and an EEPROM, which holds management information of recorded data, as shown in figure 4.

Table 1 shows contents of the information held in the storage part 112, in which numeral 114 denotes a title, numeral 115 denotes a decryption key part holding a decryption key in case of encryption in the unit of a title, and numeral 116 denotes the-number-of-digital-output-restriction-times information as information for restricting the digitally outputted number of times of recorded data.

Table 1

114		
	Title	Program A ···

115	Decryption key	Key A ···
116	The-number-of-digital-output-restriction-times information	5 ···

Figure 5 is a block diagram of the recording and reproduction apparatus 200 for recording data onto the disk medium 100 or reproducing recorded data as shown in figure 3(a). In figure 5, numeral 201 denotes a signal processing part, numeral 202 denotes a medium management part for managing read/write of data onto the disk medium 100, numeral 203 denotes a CPU which controls a data signal and control signal in the recording and reproduction apparatus 200, numeral 204 denotes a digital interface for performing two-way data communication with an external recording and reproduction apparatus 212 as an external device connected to the recording and reproduction apparatus 200 by a connection cable 213, and numeral 205 denotes a D/A converter which converts digital data into analog data to output the data.

Numeral 206 denotes a user setting part for a user to operate the recording and reproduction apparatus 200, numeral 207 denotes a display part, which is a user interface too, for displaying an operation of the recording and reproduction apparatus 200, numeral 208 denotes an optical pickup 200 which records or reproduces data onto/from the disk medium 100, numeral 209 denotes an A/D converter which converts inputted

analog data into digital data, and numeral 211 denotes a random number part which generates a key to be employed in a cipher part 210.

Here, a description will be given, provided that data of the-number-of-digital-output-restriction-times information 116 of the semiconductor tip 101 are "0" when they are not set, while the data, when set, are counted down for each digital copy and the digital copy is not permitted when its value is "1", and when digital copy is permitted only once, the value is set to "2", for example. Further, recording and reproduction of a content on/from the disk media 100 is performed in the unit of a title.

As shown in figure 6, Steps Z1 and Z3 are performed in the recording and reproduction apparatus 200 and Step Z2 is performed in the semiconductor tip 101, and they are performed in the order of Steps Z1-Z3.

That is, in Step Z1 shown in figure 7, in Step A201, when disk medium 100 is arranged in the recording and reproduction apparatus 200 as shown in figure 3, the CPU 203 detects a title and arrangement of data recorded by a user, a vacant area, and the like on the disk medium 100, by the optical pickup 208 accessing the TOB area 104 on the disk media 104, and displays the title on the display part 207.

Next, in Step A202, a title of content data to be recorded by a user, the-number-of-digital-output-restriction-times

information, presence or absence of encryption of the content are set into the user setting part 206 (here, title: program A, the-number-of-digital-output-restriction-times information: 5, and encryption: presence).

In Step A203, the CPU 203 transfers the title and the-number-of-digital-output-restriction-times information to the medium management part 202 based on the information set in the user setting part 206, and a random number is generated from the random number part 211 to create an encryption key (key A). In Step A204, the program A as analog data is inputted to the A/D converter 209, where it is converted into digital data, is further transmitted to the signal processing part 201, where the program A is made into a record format, is transmitted to the cipher part 210, where the program A is encrypted employing the key A, and is transmitted to the optical pickup 208, and the encrypted program A is recorded in a vacant area of the recording data area 102 on the disk medium 100 and a title of the recorded data and arrangement of data in the disk medium 100 are recorded in the TOB area 104 from the optical pickup 208 by a control of the CPU 203.

In Step A205, the medium management part 202 transmits a registration command, the title (program A), the-number-of-digital-output-restriction-times information (5), and the key A to the semiconductor tip 101 through the data lines.

In figure 8 as a process in Step Z2, in Step A208, the

registration command, the title (program A), the-number-of-digital-output-restriction-times information (5), and the key A are received by the I/O 110.

In Step A209, by the registration command received by the I/O 110, the CPU 111 transmits the received information in Step A208 to the storage part 112, where the information is stored as shown in Table 1.

In Step A210, an end of communication is transmitted to the medium management part 202 after recording.

In figure 9 as a process in Step Z3, the end of communication is received in step A213 and the operation for recording setting information onto the disk medium is ended.

In this way, writing of a content onto the disk medium is performed.

Next, an operation for reproducing the disk medium 100 on which a content is recorded being encrypted in the recording and reproduction apparatus 200 will be described with reference to figures 10 to 14.

As shown in figure 10, Steps A1 and A3 are performed in the recording and reproduction apparatus 200 and Steps A2 and A4 are performed in the semiconductor tip 101, and they are performed in the order of Steps A1-A4.

First, in figure 11 as a process in Step A1, in Step A401, when the disk medium 100 is arranged in the recording and reproduction apparatus 200 as shown in figure 3, the CPU 203

detects a title and arrangement of data recorded by a user, a vacant area, and the like on the disk medium 100, by the optical pickup 208 accessing the TOB area 104 on the disk media 100, and displays the title on the display part 207.

Next, in Step A402, presence or absence of output of a title to be reproduced by a user from the digital interface 204 to the external recording and reproduction apparatus 212 through the connection cable 213 is set into the CPU 203 through the user setting part 206 (title: program A, digital output: presence).

In Step A403, the CPU 203 transmits a start command indicating reproduction start, the title to be reproduced, and the information of presence or absence of digital output from the medium management part 202 to the semiconductor tip 101 through the data lines 108 and 105.

In figure 12 as a process in Step A2, the semiconductor tip 101 receives the information set in Step A402 at the I/O 110 and the CPU 111 confirms the start command in Step A406, and presence or absence of digital output is confirmed in Step A407. When there is no digital output (no), the processing proceeds to Step A409, where a decryption key (key A) selected from the decryption key part 115 of the storage part 112 according to the title (program A) is transmitted to the recording and reproduction apparatus 200.

On the other hand, when there is digital output (yes) in

the step A407, the processing proceeds to Step A408, where the-number-of-digital-output-restriction-times information 116 of the semiconductor tip 101 is compared with "2", and when the-number-of-digital-output-restriction-times information 116 is equal to or larger than "2" (yes), the decryption key (key A) selected from the decryption key part 115 of the storage part 112 according to the title (program A) is transmitted to the recording and reproduction apparatus 200 in Step A409.

When the-number-of-digital-output-restriction-times information 116 is under "2" (no) in Step A408, a reproduction non-permission command for refusing transmission of the decryption key to reproduce a content is transmitted to the recording and reproduction apparatus 200 in Step A410, and communication is ended in Step A411.

In figure 13 as a process in Step A3, the decryption key in Step A409 or the reproduction non-permission command in Step A410 is received in Step A414, and in case of reproduction non-permission command (yes) when the reproduction non-permission command is confirmed in Step A415, the processing proceeds to Step A416, where modification of the set information in Step A402 is prompted visually or aurally in the display part 207.

Here, the set information in Step A402 cannot be modified after the end of Step A403, and thus the set information is erased and setting is reattempted from Step A402 in case of modification. Therefore, even when digital output is set to

"absence" in Step A402 and is modified to "presence" after the end of Step A402, unjustified digital output of a content which cannot be digitally outputted can be prevented by Step A408.

On the other hand, in case of no reproduction non-permission command (no) in Step A415, the processing proceeds to Step A417, where presence or absence of digital output set in Step A402 is confirmed, and in case of "presence" (yes), the processing proceeds to Step A418, where a content of the title (program A) set in Step A402 is reproduced employing the decryption key (key A) received in Step A414 and decrypted data are outputted from the digital interface 204 in digital format, and a reproduction end is transmitted to the semiconductor tip 101 when the reproduction is ended in Step A419.

In Step A417, when presence of absence of digital output set in Step A402 is confirmed and it is "absence" (no), the processing proceeds to Step S420, where the content of the title (program A) set in Step A402 is decrypted employing the decryption key (key A) received in Step S414 and is reproduced in analog format from the D/A converter 205.

In figure 14 as a process in Step A4, when the semiconductor tip 101 receives a reproduction end at the I/O 110 and the CPU 111 confirms the reproduction end in Step A423, the-number-of-digital-output-restriction-times information 116 is updated to the number of times which is obtained by subtracting "1" from the-number-of-digital-output-restriction-

times information 116 of the storage part 112, "5 - 1 = 4", in Step A424, and it is recorded to end reproduction of the content.

As described above, according to the first embodiment, the semiconductor tip 101 is provided in the disk medium 100 as a content recording medium and the information for restricting the number of digital output times is held and managed in the semiconductor tip 101, whereby the number of digital output times such as digital copy of a content can be restricted, the semiconductor tip 101 is embedded in the disk medium 100, whereby the semiconductor tip 101 is not copied even when a content storage area is physically copied by such a method as a stamp copy, and a content is encrypted so as to be decrypted only by a key stored in the semiconductor tip 101, whereby contents of the content are not taken out to the outside in a reproducible state.

Further, the-number-of-digital-output-restriction-times information 116 is updated after a reproduction end of a content is confirmed in Step A423, whereby digital output of the content can be assured even when digital output is stopped in process of reproduction due to some trouble.

(Embodiment 2)

Next, a data recording medium and data management system according to a second embodiment of the present invention will be described. In the second embodiment, a description will be

given of a case where a reproduction operation being provided with plural digital data input/output openings is employed, while the first embodiment is described as a case of one interface.

Figure 15 is a diagram illustrating a constitution of a semiconductor tip 101a, in which numeral 113 denotes a digital output number holding means (output path number storage part) for holding the number of digital outputs to the outside in case of digitally outputting to the outside of an apparatus for reproducing recorded data. Here, the same reference numerals as those shown in figure 4 denote the same or corresponding parts.

Figure 16 is a block diagram of a recording and reproduction apparatus, which holds the operation in figure 3(a) that enables reproduction of recorded data on a disk medium 100. In the figure, numeral 300 denotes a recording and reproduction apparatus, numeral 301 denotes a digital interface (A), numeral 302 denotes a digital interface (B) having plural digital output/input openings, numeral 202 denotes a hard disk (HDD) device (A), and numeral 304 denotes a hard disk (HDD) device (B). The same reference numerals as those shown in figure 5 denote the same or corresponding parts.

The so-constituted recording and reproduction apparatus 300 will be described with reference to figures 17 to 21.

To reproduce a content on the disk medium 100, Steps B1

and B3 are performed in the recording and reproduction apparatus 300 and Steps B2 and B4 are performed in the semiconductor tip 101a, and they are performed in the order of Steps B1-B4, as shown in figure 17.

In figure 18 as a process in Step B1, in Step B601, when the disk medium 100 is arranged in the recording and reproduction apparatus 300 as in figure 3, the CPU 203 confirms a title and arrangement of data recorded by a user, a vacant area, and the like on the disk medium 100, by the optical pickup 208 accessing the TOB area 104, and displays the title on the display part 207.

Next, in Step B602, a title to be reproduced by a user is selected in the user setting part 206 when it is digitally outputted from the digital interfaces (A) 301 and (B) 302 to the external recording and reproduction apparatus 212 and the HDD devices (A) 303 and (B) 304 through the connection cable 213, and the number of digital outputs is set in the CPU 203 through the user setting part 206 (title: program A, digital output: 3), and a start command indicating reproduction start, the title to be reproduced, and the number of digital outputs are transmitted to the semiconductor tip 101a in Step B603. Here, when there is no digital output in Step B602, a description will be given as "0".

In figure 19 as a process in Step B2, the information set in Step B602 is received and the start command is confirmed in

Step B606, and the digital output number is compared with "0", so that presence or absence of digital output is detected in Step B607. In case of digital output number being "0" (no) in Step B607, digital output is considered to be "absence" and the processing proceeds to Step B614, where a decryption key (key A) selected from the decryption key part 115 according to the title is transmitted to the recording and reproduction apparatus 300.

On the other hand, in case of digital output number being other than "0" (yes) in Step B607, digital output is considered to be "presence" and the processing proceeds to Step B608, where the-number-of-digital-output-restriction-times information 116 is compared with "2", so that it is detected whether digital output is possible.

When the-number-of-digital-output-restriction-times information 116 is under "2" (no) in Step B608, the processing proceeds to Step B611, where a reproduction non-permission command for refusing transmission of the decryption key to reproduce a content is transmitted to the semiconductor tip 101a. On the other hand, when the-number-of-digital-output-restriction-times information 116 is equal to or larger than "2" (yes) in Step B608, Step B609 is executed.

In Step B609, where the digital output number is compared with "2", when the digital output number is under "2", that is, "1" or less (no), the digital output number is set in the

digital output number holding part 113 in Step B613, and the decryption key (key A) selected from the decryption key part 115 according to the title (program A) is transmitted to the recording and reproduction apparatus 300 in Step B614.

When the digital output number is over "2" (yes) in Step B609, the processing proceeds to Step B610, where the result of subtracting the digital output number from the-number-of-digital-output-restriction-times information 116 is compared with "1", and when the result of subtracting the digital output number from the-number-of-digital-output-restriction-times information 116 is under "1" (yes), a reproduction non-permission command for refusing transmission of the decryption key to reproduce a content is transmitted to the semiconductor tip 101a in Step B611, and communication is ended in Step B612.

On the other hand, when the result of subtracting the digital output number from the-number-of-digital-output-restriction-times information 116 is equal to or larger than "1" (no) in Step B610, the processing proceeds to Step B613, where the digital output number is set in the digital output number holding means 113 (3), and the decryption key (key A) selected from the decryption key 115 according to the title (program A) is transmitted to the recording and reproduction apparatus 300 in Step B614.

In figure 20 as a process in Step B3, the reproduction non-permission command in Step B611 or the decryption key in

Step B614 is received in Step B617, whether what is received is the reproduction non-permission command or not is confirmed in Step B618, and in case of this being the reproduction non-permission command (yes), the processing proceeds to Step B619, where modification of the set information in Step A602 is prompted visually or aurally in the display part 207.

On the other hand, when what is received is judged not to be the reproduction non-permission command (no) in Step B618, the processing proceeds to Step B620, where the digital output number is compared with "0", so that presence or absence of digital output is detected.

When the digital output number is "0" (no) in Step B620, the digital output is considered to be "absence", and a content of the title (program A) set in Step B602 is reproduced employing the decryption key (key A) received in Step B617 and is outputted in only analog format from the D/A converter 205 in Step B623.

On the other hand, when the digital output number is other than "0" (yes) in Step B620, the digital output number is considered to be "presence", and a content of the title (program A) set in Step B602 is reproduced employing the decryption key (key A) received in Step B617 and is outputted from the digital interface (A) 301 or the digital interface (B) 302 in digital format, and a reproduction end is transmitted to the semiconductor tip 101a when the reproduction is ended in

Step B622.

In figure 21 as a process in Step B4, confirmation of a reproduction end is performed in Step B626, and in case of reproduction end, the processing proceeds to Step B627, where the digital output number holding means 113 (3) is subtracted from the-number-of-digital-output-restriction-times information 116 to update the-number-of-digital-output-restriction-times information 116 and the updated number of times is stored, and reproduction of a content is ended.

As described above, according to the second embodiment, in the recording and reproduction apparatus provided with plural digital output openings, a function of holding the number of digital outputs is provided in the semiconductor tip 101a in the disk medium 100, and the value of the digital output number holding means 113 is subtracted from the-number-of-digital-output-restriction-times information 116 when a digital copy is ended, whereby it is possible to restrict the number of copy times when a reproduced content is digitally copied simultaneously employing plural digital outputs.

(Embodiment 3)

Next, a data recording medium and data management system according to a third embodiment of the present invention will be described. In the third embodiment, the semiconductor tip 101b is provided with a function of permitting reproduction of a disk medium by performing user authentication employing

user's personal information (password) in addition to the construction of the first and second embodiments. Here, a description will be given exemplifying a case where the function of the third embodiment is applied to the first embodiment.

Figure 22 is a block diagram illustrating a constitution of the semiconductor tip 101b in the third embodiment, in which numeral 117 denotes a personal information holding part (personal information storage part) for holding a password aimed at user authentication. Other parts are the same as those shown in figure 4, and their descriptions will be omitted here.

An operation of the so-constituted third embodiment will be described with reference to figures 23 to 27. Here, a description will be given, provided that personal information is not registered when the value of the personal information holding part 117 is "0", the disk medium 100 is arranged in an apparatus to record or reproduce, the CPU 111b of the semiconductor tip 101b confirms the personal information holding part 117 at the point of time when power is applied, and an access to the storage part 112 is restricted unless personal information inputted from the recording and reproduction apparatus 200 matches the personal information, when it is set (to other than 0).

First, an operation for registering personal information

for authenticating a user in the semiconductor tip 101b by the recording and reproduction apparatus 200 will be described.

As shown in figure 23, Steps C1 and C3 are performed in the recording and reproduction apparatus 200 and Steps C2 and C4 are performed in the semiconductor tip 101b, and they are performed in the order of Steps C1-C4.

In figure 24 as a process in Step C1, by arranging the disk medium 100 in the recording and reproduction apparatus 200, the CPU 203 transmits personal information confirmation command for confirming presence or absence of registration of personal information in the disk medium 100 in Step C801.

Next, in figure 25 as a process in Step C2, the personal information confirmation command is received in Step C804, the CPU 111b compares the personal information holding part 117 with "0" in order to confirm presence or absence of personal information according to the personal information confirmation command in Step C805, and in case of the personal information holding part 117 being "0" (no), which results in "no personal information", the processing proceeds to Step C807, where a no-personal-information command is transmitted. On the other hand, when the personal information holding part 117 is not "0" (yes) in Step C805, which results in "personal information", the processing proceeds to Step C806, where a personal information command is transmitted.

In figure 26 as a process in Step C3, the personal

information command or the no-personal-information command is received in Step C811, the CPU 203 confirms whether or not it is no-personal-information command in Step C812, and in case of no-personal-information command detected (yes), the processing proceeds to Step C813, where a reproduction operation is performed or a registration command for registering personal information and the personal information to be registered are inputted from the user setting part 206 and are transmitted to the semiconductor tip 101b. An operation when other than the no-personal-information command is detected (no) in Step C812 will be described in an after-mentioned user authentication operation.

In figure 27 as a process in Step C4, the registration command and the personal information to be registered are received in Step C817, and the CPU 111b stores the personal information in the personal information holding part 117 based on the registration command in Step C818.

Next, an operation of the recording and reproduction apparatus 200, when personal information for performing user authentication is registered in the semiconductor tip 101b, will be described with reference to figures 28 to 31.

As shown in figure 28, Steps C1, D3, and D5 are performed in the recording and reproduction apparatus 200 and Steps C2 and D4 are performed in the semiconductor tip 101b, and they are performed in the order of Steps C1-D5. Here, the same step

names as those in figures 23 to 27 denote the same processes, and their descriptions will be omitted.

In figure 29 as a process in Step D3, personal information command or no-personal-information command is received in Step D1011, the CPU 203 confirms whether or not it is no-personal-information command in Step D1012, and in case of other than no-personal-information command (no), input of personal information to the display part 207 is promoted in Step D1014, and a personal information command as a confirmation command of the personal information and inputted personal information are transmitted to the semiconductor tip 101b in Step D1015, when the personal information is inputted.

In figure 30 as a process in Step D4, the personal information command and the inputted personal information are received in Step D1018, the CPU 111b compares the personal information in the personal information holding part 117 with the inputted personal information based on the personal information command in Step D1019, and in case of these matching (yes), the processing proceeds to Step D1020, where a continuation command informing establishment of user authentication is transmitted, while in case of mismatch (no), the processing proceeds to Step D1021, where a communication end is transmitted.

Here, user authentication is established in case of (yes) in Step D1019 and the CPU 111b is subsequently operated to

access the storage part 112, thereby enabling a recording or reproduction operation onto the disk medium 100.

In figure 31 as a process in Step D5, the continuation command or the communication end is received in Step D1024, the CPU 203 confirms whether or not it is continuation command in Step D1025, and when it is judged to be a continuation command (yes) here, the processing proceeds to Step D1026, where a recording or reproduction operation onto the disk medium 100, issue of an erasing command as a command for erasing information of the personal information holding part 117, or transmission of a registration command for modifying registered personal information or the like are possible.

On the other hand, when it is judged not to be the continuation command (no) in Step D1025, the processing proceeds to Step D1027, where communication is ended.

Further, it is also possible that plural pieces of personal information are provided in the personal information holding part 117, a user selects his/her personal information of the personal information holding part 117, and the above-described operation is performed plural times.

In addition, it is also possible that user authentication information is set in unit of the title registered in the storage part 112 of the semiconductor tip 101b and reproduction is made possible only when user authentication is established.

As described above, according to the third embodiment,

user's personal information (password) is stored in the semiconductor tip 101b in the disk medium 100 and authentication is performed at medium reproduction, so that user authentication is possible on the side of disk medium, whereby such actions as an unjustified copy of the disk medium 100 by a third person can be prevented, resulting in firm security of a content.

(Embodiment 4)

Next, a data recording medium and data management system according to a fourth embodiment of the present invention will be described. The fourth embodiment is provided with a function of detecting an unjustified operation with respect to user authentication when personal information is set in a personal information holding part of a semiconductor tip in addition to the construction of the third embodiment. That is, figure 32 is a block diagram illustrating a constitution of a semiconductor tip 101c in the fourth embodiment, in which numeral 118 denotes the-number-of-unjustification-times holding part (the-number-of-mismatch-times holding part) for holding the number of mismatch times of confirmation of personal information (password). Other parts are the same as those shown in figure 22, and their descriptions will be omitted here.

Here, a description will be given, provided that in the-number-of-unjustification-times holding part 118, arbitrary value other than "0" is set, which value is set by clearing a

stored value, and an unjustified access is considered to be detected when "0" is held in the-number-of-unjustification-times holding part 118.

Hereinafter, a description will be given with reference to figures 33 to 35 mainly of an operation for detecting an unjustified access for analyzing personal information or the like, when the personal information for user authentication is registered in the semiconductor tip 101c.

As shown in figure 33, Steps C1, D3, and E5 are performed in the recording and reproduction apparatus 200 and Steps C2 and E4 are performed in the semiconductor tip 101c, and they are performed in the order of Steps C1-E5. Here, the same step names as those in figure 28 denote the same processes, and their descriptions will be omitted.

First, in figure 34 as a process in Step E4, personal information command and input personal information are received in Step E1101.

Next, the CPU 111c compares memory contents of the-number-of-unjustification-times holding part 118 with "0" in Step E1102, and in case of the memory contents of the-number-of-unjustification-times holding part 118 being "0" (yes), the processing proceeds to Step E1103, where an unjustified action is considered to exist and an unjustified access command is transmitted to the recording and reproduction apparatus 200.

On the other hand, when the memory contents of the-number-

of-unjustification-times holding part 118 are other than "0" (no) in Step E1102, the processing proceeds to Step E1104, where the CPU 111c compares the personal information holding part 117 and the input personal information based on the personal information command, and in case of matching as a result (yes), the processing proceeds to Step E1105, where the-number-of-unjustification-times holding part 118 is cleared and a prescribed value other than "0" is set therein, and a continuation command informing establishment of user authentication is transmitted in Step E1106. On the other hand, in case of mismatch (no) in Step E1104, the processing proceeds to Step E1107, where the result obtained by subtracting "1" from a value stored in the-number-of-unjustification-times holding part 118 is held as the-number-of-unjustification-times holding part 118, and a communication end is transmitted to the recording and reproduction apparatus 200 in Step E1108.

When user authentication is established before the value set in the-number-of-unjustification-times holding part 118 is "0" by executing Step E1105, the-number-of-unjustification-times holding part 118 is cleared and returned to the prescribed value. Therefore, even when the number of unjustification times is recorded due to user's incorrect input, correct input is performed again and the number of unjustification times due to incorrect input is counted, thereby preventing access onto the disk medium from abruptly

becoming impossible by accumulation of the number of unjustification times due to incorrect input. Further, when a person other than a user successively inputs information which is not stored in the personal information holding part 117 in order to perform unjustified user authentication, the value of the-number-of-unjustification-times holding part 118 approximates "0", and existence of unjustified access can be detected when the-number-of-unjustification-times holding part 118 is "0".

In figure 35 as a process in Step E5, one of an unjustified access command, a continuation command, and a communication end is received in Step E1111, the CPU 203 confirms whether the received information is unjustified access command or not in Step E1112, and in case of unjustified access command (yes), the processing proceeds to Step E1113, where existence of an unjustified action is displayed visually or aurally in the display part 207.

On the other hand, when the CPU 230 confirms information other than the unjustified access command (no) in Step E1112, the processing proceeds to Step E1114, where the CPU 230 confirms whether the information is continuation command or not, and in case of continuation command (yes), the processing proceeds to Step E1115, where a recording or reproduction operation onto the disk medium 100, issue of an erasing command as a command for erasing information of the personal

information holding part 117, transmission of a registration command for modifying registered personal information, or the like are possible.

When the CPU 203 judges it is not the continuation command (no) in Step E1114, the processing proceeds to Step E1116, where communication is ended.

As described above, according to the fourth embodiment, by a function of storing the number of unjustified access times being provided with the semiconductor tip 101c of the disk medium 100, it is possible, for example, to record and hold on the side of the disk medium 100 that a third person performed an unjustified access to the disk medium 100 viciously, whereby it is possible to warn a regular owner of the disk medium 100 of an unjustified access.

Further, the reproduction apparatus may stop an unjustified action by intimidating with a loud sound or the like when an unjustified access is detected.

(Embodiment 5)

Next, a data recording medium and data management system according to a fifth embodiment of the present invention will be described. In the fifth embodiment, an authenticating operation employing a cipher is performed in the above-described respective embodiments. Here, a description will be given exemplifying a case where this embodiment is applied in the first embodiment.

Figure 36 is a block diagram illustrating a constitution of a semiconductor tip 101d in the fifth embodiment, in which numeral 119 denotes a cipher part of the recoding and reproduction apparatus 200, which has the same cipher algorithm as that of the cipher part 210, numeral 120 denotes a random number part which generates a random number, and numeral 121 denotes a key box part as a set of key arrangement employed in the cipher part 119. Other parts are the same as those shown in figure 4, and their descriptions will be omitted here. Figure 37 is a block diagram of a recording and reproduction apparatus 400 in the fifth embodiment, in which numeral 214 denotes a key box part having the same function as that of the key box part 121 included in the semiconductor tip 101d mounted on the disk medium 100. The same reference numerals as those shown in figure 5 denote the same or corresponding parts.

Table 2 shows information held in the key box part 121 and the key box part 214, in which numeral 1700 denotes a key code for selecting a key and numeral 1701 denotes a key selected according to the key code 1700.

Table 2

1700 Key code	1701 Key
Key code 1	Key KC1
Key code 2	Key KC2
.	.
.	.

An authenticating operation in the so-constituted

semiconductor tip 101d in the disk medium 100 and recording and reproduction apparatus 400 will be described with reference to figures 38 to 41. As shown in figure 38, Steps G1, G3, and G5 are performed in the recording and reproduction apparatus 400 and Steps G2 and G4 are performed in the semiconductor tip 101d, and they are performed in the order of Steps G1-G5.

Data encryption and decryption are subsequently described as follows.

Function name = E/D (A, B)

Provided that E/D = E: encryption and D = decryption, A denotes a key in encryption or decryption and B denotes a plain text or a cipher text.

To generate a cipher text C by encrypting the plain text B by the key A, for example,

C = E (A, B).

Decryption is

B = D (A, C).

In figure 39 as a process in Step G1, an authentication start command is transmitted to the semiconductor tip 101d in Step G1801.

In figure 40 as a process in Step G2, the authentication start command is received in Step G1804, the CPU 111d generates a random number, RX, from the random number part 120 based on the authentication start command in Step G1805, "key code 1" is generated employing a list of the random number RX and "key

KC1" is selected from the "key code 1" at the key box part 121 in Step G1806, the random number RX is subjected to encryption: E1 = E (KC1, RX) with the "key KC1" as a key at the cipher part 119 so as to create E1 in Step G1807, and the E1 and the "key code 1" are transmitted to the recording and reproduction apparatus 400 in step G1808.

In figure 41 as a process in Step G3, the E1 and the "key code 1" are received in Step G1811, the CPU 203 selects the "key KC1" corresponding to the "key code 1" at the key box part 214 in Step G1812, and the E1 is subjected to decryption: D1 = D (KC1, E1) with the "key KC1" as a key at the cipher part 210 so as to create D1 in Step G1813.

Next, a random number is generated at the random number part 211 and "key code 2", which is different from the "key code 1", is generated employing a list of the random number in Step G1814, a key is selected as "key KC2" from the key box part 214 by the "key code 2" in Step G1815, the D1 is subjected to encryption: E2 = (KC2, D1) with the "key KC2" as a key at the cipher part 210 so as to create E2 in Step G1816, the E2 and the "key code 2" are transmitted to the semiconductor tip 101d in Step G1817, and the D1, the "key KC1", and the "key KC2" are subjected to exclusive OR: KI1 = D1 . KC1 . KC2 (. is a mark denoting exclusive OR), so as to create "KI1" as a transmission key employed as a key for encrypting and transmitting data required for recording or reproduction in

Step G1818.

In figure 42 as a process in Step G4, the E2 and the "key code 2" are received in Step G1821, the CPU 111d selects the "key KC2" corresponding to the "key code 2" at the key box part 121 in step G1822, the E2 is subjected to decryption: D2 = (KC2, E2) with the "key KC2" as a key at the cipher part 119 so as to create D2 in Step G1823, the random number RX and the D2 are compared in Step G1824, and in case where the random number RX mismatches the D2 (no), the processing proceeds to Step G1827, where a communication end is transmitted, and transmission is ended in Step G1828.

On the other hand, in case where the random number RX matches the D2 in Step G1824 (yes), the semiconductor tip 101d authenticates the recording and reproduction apparatus 400, and the RX, the "key KC1", and the "key KC2" are subjected to exclusive OR: KI2 = RX . KC1 . KC2, so as to create "KI2" as a transmission key employed as a key for encrypting and transmitting data required for recording or reproduction in Step G1825, and a continuation command is transmitted in Step G1826.

In figure 43 as a process in Step G5, the continuation command or the transmission end is received in Step G1531, it is confirmed whether the received information is a continuation command or not in Step G1532, and in case where this is judged not to be a continuation command (no), the processing proceeds

to Step G1534, where communication is ended, while in case where this is judged to be a continuation command, the processing proceeds to Step G1533, where a reproduction operation is performed.

As described above, according to the fifth embodiment, a cipher processing function is provided with the semiconductor tip 101d of the disk medium 100 and authentication is performed employing a cipher, whereby reproduction of the disk medium 100 is permitted only in the environment enabling cipher communication, resulting in further enhancement in content security.

Further, a transmission key for encrypting and transmitting data required for a recording or reproduction operation is generated differently for each authentication, employing data in communication process including random number data, whereby a high-security key can be created.

While in the first embodiment, the semiconductor tip 101 which the pins 133 is connected to is embedded in the base material part 131 with a concave portion and both sides thereof are applied with the recording layers 132, thereby to manufacture the disk medium 100, it is also possible that only a part of the clipping area 103 having the semiconductor tip 101 and the wiring 105 is created separately and is embedded in the disk medium 100, which has the outside of the clipping area 103 created conventionally.

Further, while in the first embodiment, the wiring 105 is employed in the clipping area 103 so as to supply power or a signal to the semiconductor tip 101 mounted on the disk medium 100, it is also possible that a solar battery panel is mounted on the clipping area 103 to supply power to the semiconductor tip 101 as well as to irradiate a semiconductor laser to a specified position of the solar battery panel, thereby transferring a signal.

Further, while a password is held in the disk medium 100 as personal information so as to be confirmed in the third embodiment, or a cipher processing is employed to perform authentication between the disk medium 100 and the reproduction apparatus 400 in the fifth embodiment, it is also possible that an algorithm for authentication is held in a medium such as an IC card, which is employed instead of a key at content reproduction, thereby to prevent unjustified use.

APPLICABILITY IN INDUSTRY

As described above, a data recording medium and data management system according to the present invention can enhance security in copyright management in a disk medium and is highly available as one effectively preventing copyright piracy.

CLAIMS

1. A data recording medium for content recording or reproduction including:

a reproduction history management circuit which records copyright protection information and manages reproduction and output of a content referring to the copyright protection information at content reproduction.

2. The data recording medium as defined in Claim 1,

the data recording medium is made of a recording layer for recording a content and a base material layer, wherein

the reproduction history management circuit is embedded in a part of the base material layer in a clipping area in the data recording medium, and

the clipping area is an area where the data recording medium is fixed with respect to a rotation drive for rotating the data recording medium.

3. The data recording medium as defined in Claim 1 or 2, wherein

the content is encrypted employing a key and is recorded on the data recording medium, and

the reproduction history management circuit comprises: a

storage part for storing a decryption key for decrypting the content recorded on the data recording medium; and

a content output management part for restricting the number of output times of the decrypted content in digital format when a content is reproduced from the data recording medium.

4. The data recording medium as defined in Claim 3, wherein

the content recorded on the data recording medium is encrypted employing a key different in unit of the title or the arbitrary data size, and

the content output management part has a decryption key for each unit of content encryption and restricts the number of output times of the content in digital format in unit of the title or the arbitrary data size.

5. The data recording medium as defined in Claim 3 or 4, wherein

when the content is outputted in digital format, the content output management part updates and records its number of times, compares the number of times with the previously set number of restriction times, and decides not to output the content in digital format when the number of output times of the content in digital format exceeds the number of restriction times.

6. The data recording medium as defined in Claim 5, wherein

when the content is outputted in digital format simultaneously through plural paths, the content output management part has an output path number storage part for storing the number of paths, and adds the number of paths stored in the output path number storage part to count outputs of the content in digital format, when the number of output times of the content in digital format is counted.

7. The data recording medium as defined in any of Claims 1 to 6, wherein

the content output management part has personal information storage part for storing personal information for authenticating an owner of the data recording medium and compares externally inputted information with the personal information and permits reproduction of the content only when the comparison results in matching, at reproduction of the content.

8. The data recording medium as defined Claim 7, wherein

the content output management part has the-number-of-mismatch-times holding part which compares the externally inputted information with the personal information and stores the number of mismatch times when the comparison successively

results in mismatch, and suppresses reproduction of the content as well as informs the outside of the mismatch when the number of mismatch times exceeds a prescribed value.

9. The data recording medium as defined in any of Claims 1 to 8, wherein

the content output management part further has a cipher processing part for performing an encryption processing according to a prescribed algorithm and performs authentication by a cipher between the data recording medium and the recording and reproduction apparatus, and suppresses reproduction of the content according to the authentication result.

10. A data management system for managing data employing a data recording medium for content recording or reproduction, wherein

the data recording medium has a reproduction history management circuit which records copyright protection information and manages reproduction and output of a content referring to the copyright protection information at content reproduction,

the recording and reproduction apparatus has a medium management part which is connected to the reproduction history management circuit and manages writing or reading of data on the data recording medium, and

when the content is reproduced, an encrypted content is decrypted by a decryption key held in the reproduction history management circuit to be reproduced, and when it is outputted in digital format, the number of output times is restricted by the reproduction history management circuit.

11. The data management system as defined in Claim 10, wherein

the recording and reproduction apparatus has plural digital output openings,

the reproduction history management circuit further records the number of paths when the content is outputted in digital format simultaneously through plural paths, and

the number of paths is added by the reproduction history circuit to restrict the number of output times, when the content is outputted in digital format through the plural paths.

12. The data management system as defined in Claim 10 or 11, wherein

the reproduction history management circuit further records personal information for recognizing an owner of the data recording medium, and

when the content is reproduced, externally inputted information is compared with the personal information held by the reproduction history management circuit, and reproduction of the content is suppressed according to the comparison result.

13. The data management system as defined in Claim 12, wherein

the reproduction history management circuit further records the number of mismatch times of a result of the comparison, and

when the content is reproduced, a previously set number of times is compared with the number of mismatch times held by the reproduction history management circuit, thereby to suppress reproduction of the content.

14. The data management system as defined in any of Claims 10 to 13, wherein

the reproduction history management circuit subjects a cipher key to an encryption processing according to a prescribed algorithm,

the medium management part subjects the cipher key to an encryption processing by the same algorithm as that of the reproduction history management circuit, and

when the content is reproduced, authentication is performed between the data recording medium and the recording and reproduction apparatus employing the encryption processing by the reproduction history management circuit and the encryption processing of the medium management part, and whether or not the content can be decrypted is judged according to the authentication result.

Fig.1

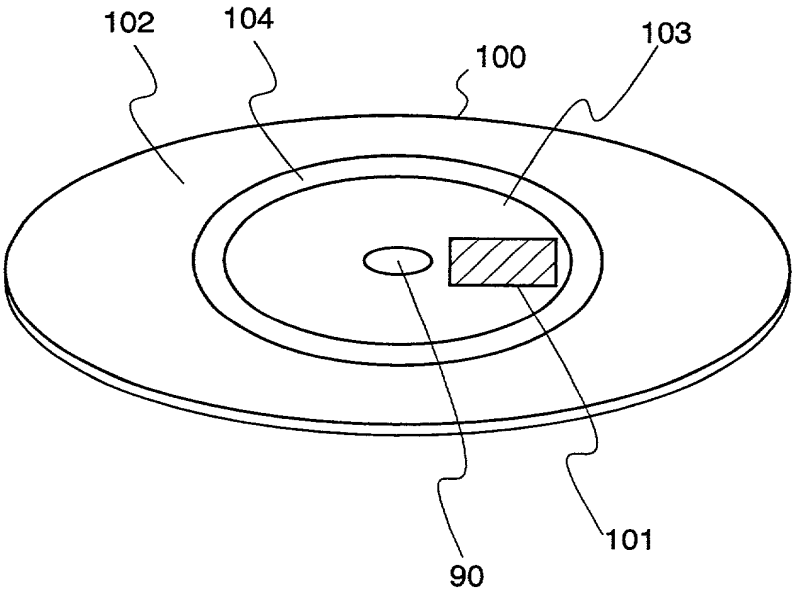

102
104
100
103
101
90

Fig.2

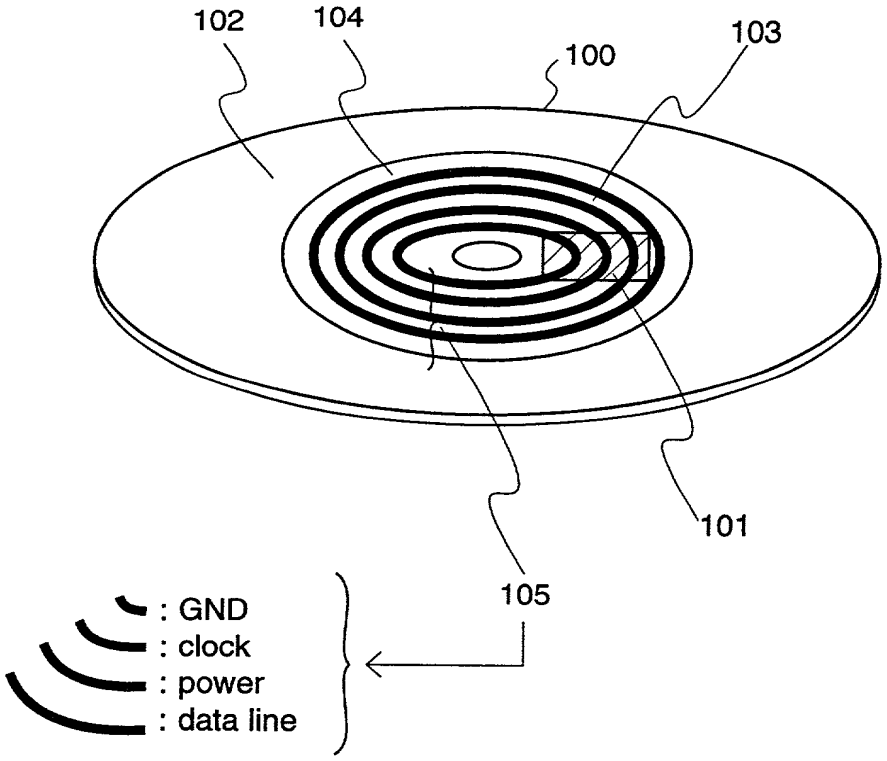

102
104
100
103
101
105
: GND
: clock
: power
: data line

Fig.3 (a)

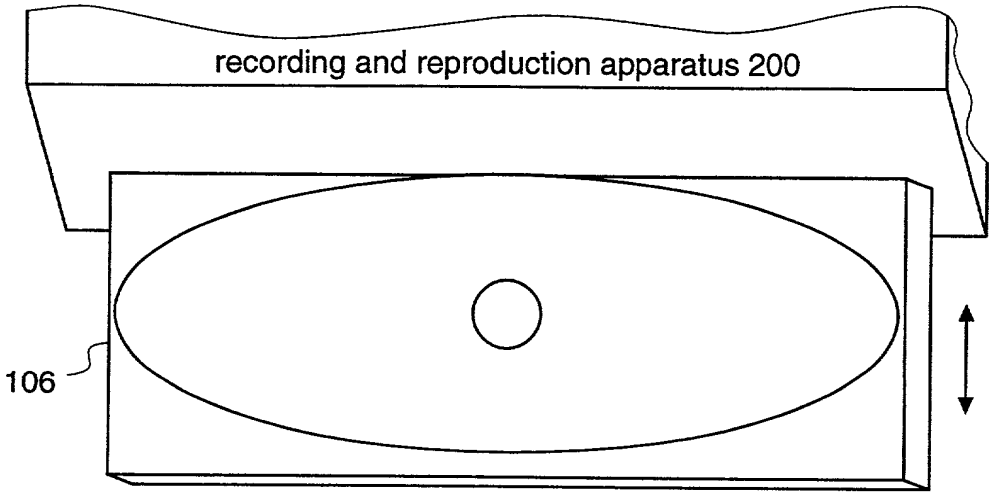


Fig.3 (b)

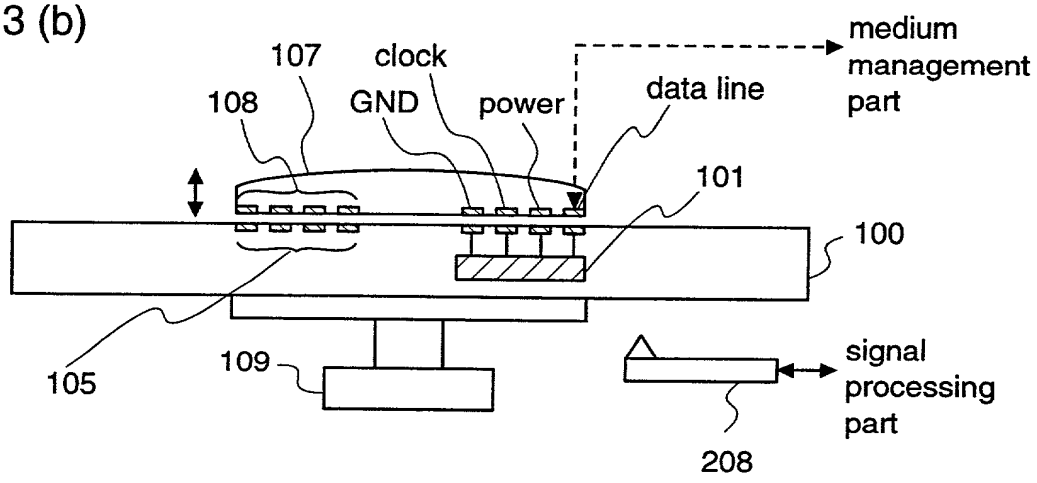


Fig.3 (c)

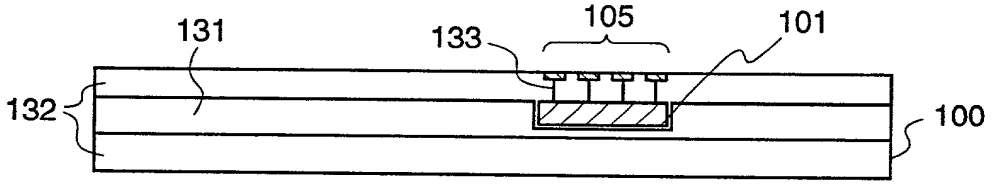
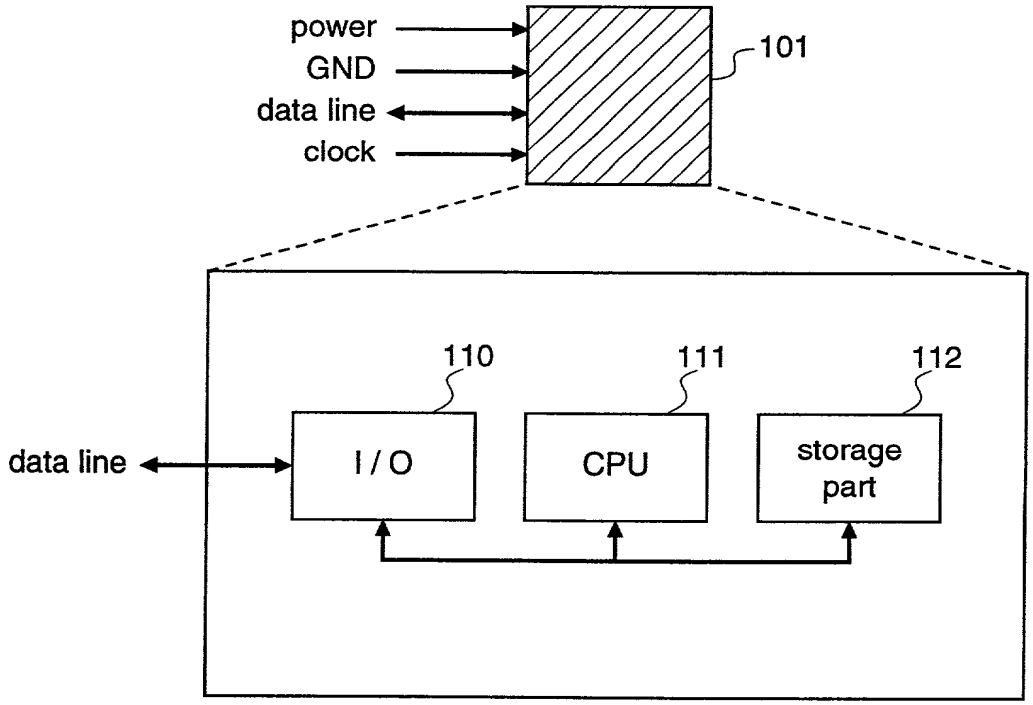


Fig.4


power
GND
data line
clock
101
110
111
112
data line
I / O
CPU
storage part

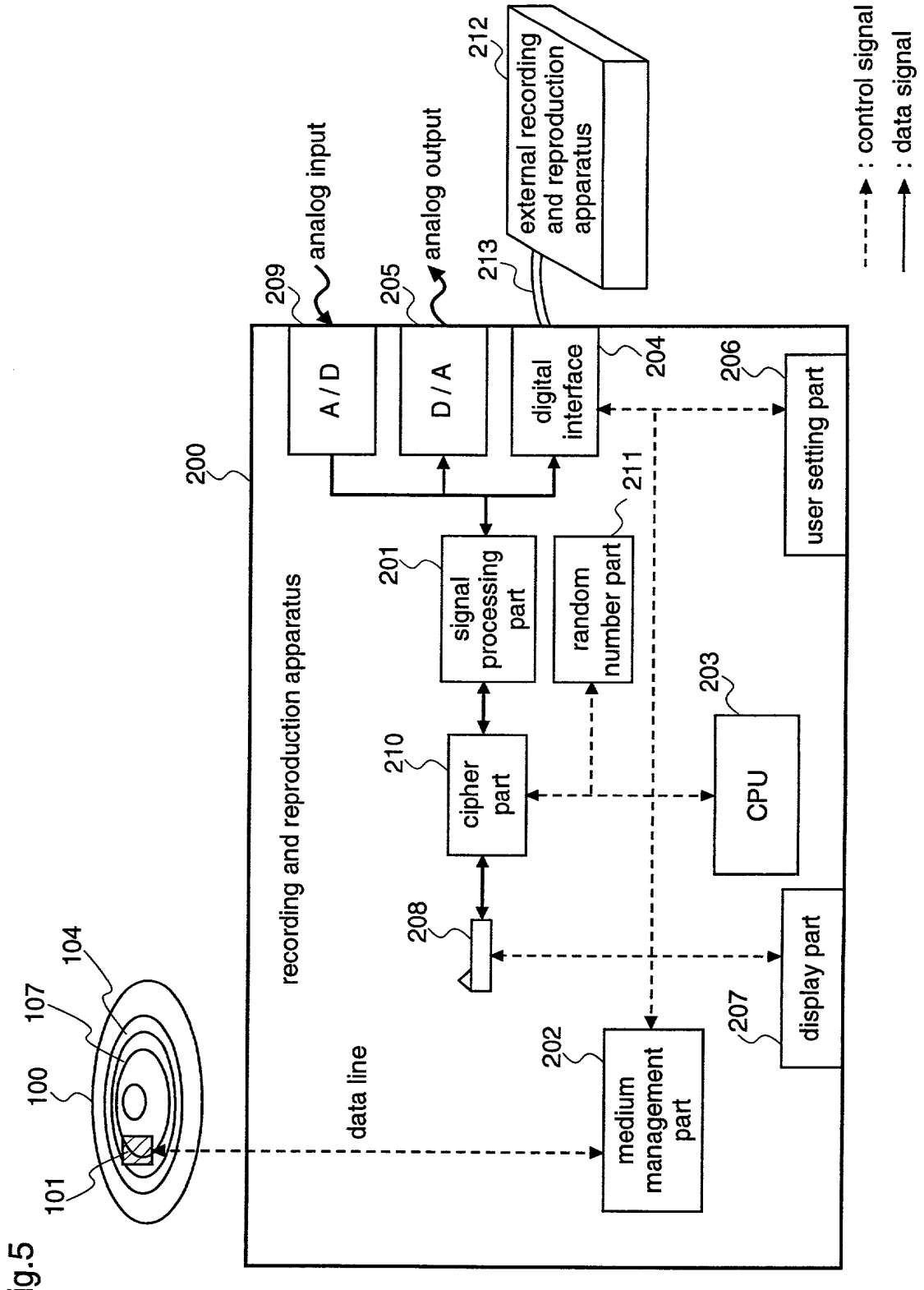

recording and reproduction apparatus
200
A / D
D / A
digital interface
204
analog input
209
analog output
205
212
external recording and reproduction apparatus
213
206
user setting part
211
random number part
201
signal processing part
210
cipher part
208
CPU
203
display part
207
medium management part
202
data line
100
101
104
107
: control signal
: data signal

Fig.5

Fig.6

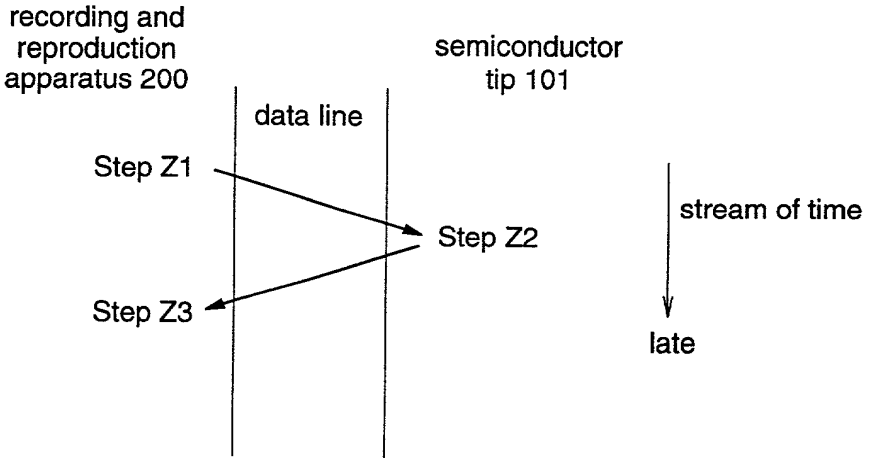

recording and reproduction apparatus 200
semiconductor tip 101
data line
Step Z1
Step Z2
Step Z3
stream of time
late

Fig.7

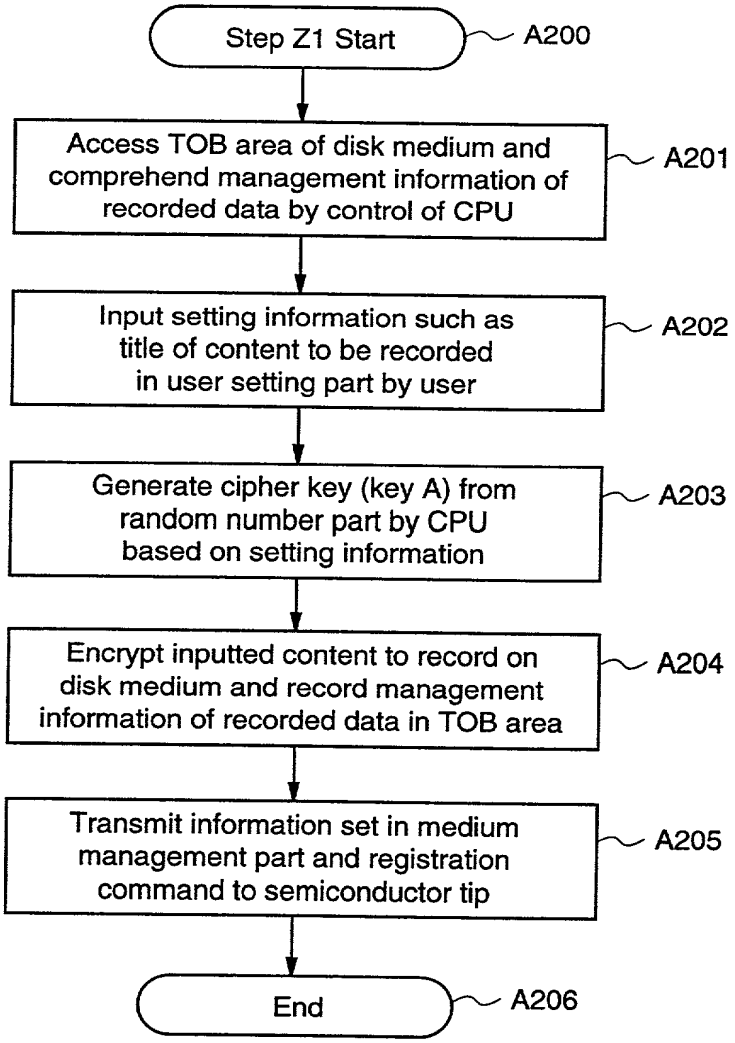

Step Z1 Start
A200
Access TOB area of disk medium and comprehend management information of recorded data by control of CPU
A201
Input setting information such as title of content to be recorded in user setting part by user
A202
Generate cipher key (key A) from random number part by CPU based on setting information
A203
Encrypt inputted content to record on disk medium and record management information of recorded data in TOB area
A204
Transmit information set in medium management part and registration command to semiconductor tip
A205
End
A206

Fig.8

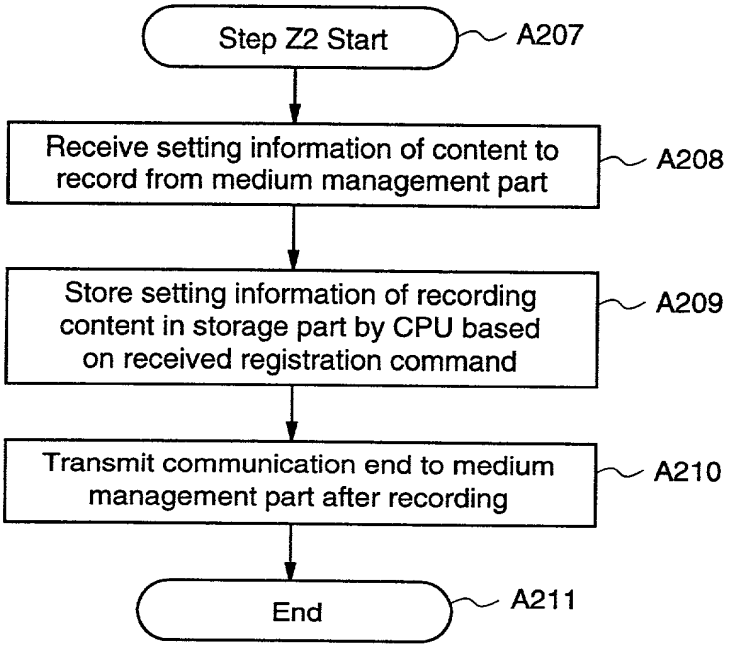

Step Z2 Start
A207
Receive setting information of content to record from medium management part
A208
Store setting information of recording content in storage part by CPU based on received registration command
A209
Transmit communication end to medium management part after recording
A210
End
A211

Fig.9

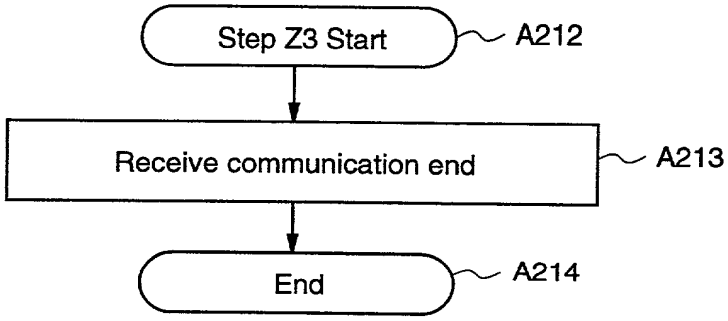

Step Z3 Start
A212
Receive communication end
A213
End
A214

Fig.10

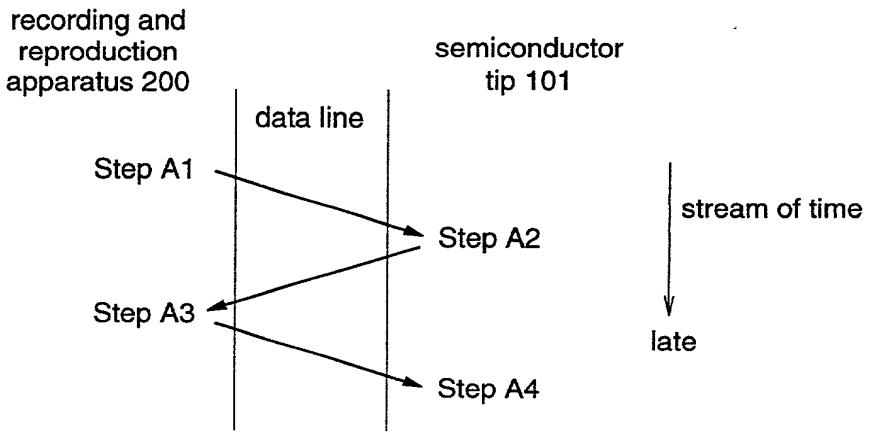

recording and reproduction apparatus 200
semiconductor tip 101
data line
Step A1
Step A2
Step A3
Step A4
stream of time
late

Fig.11

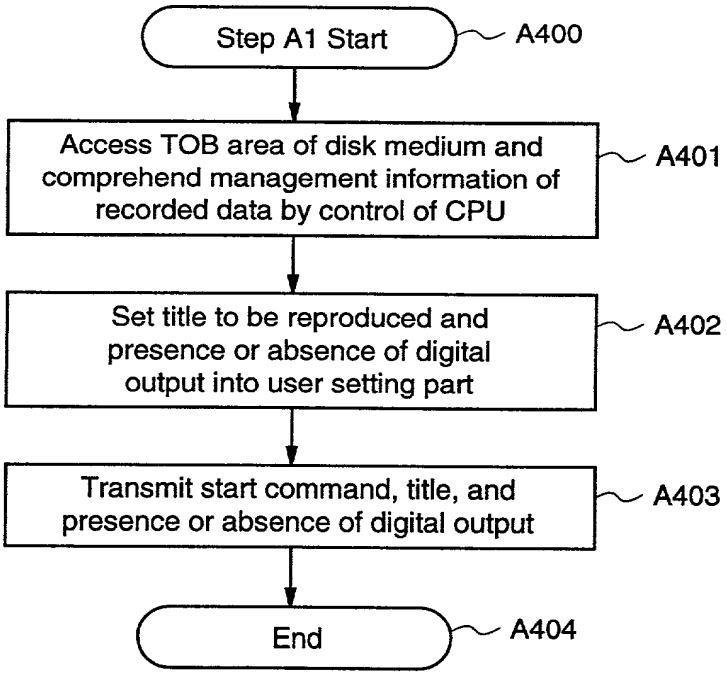

Step A1 Start
A400
Access TOB area of disk medium and comprehend management information of recorded data by control of CPU
A401
Set title to be reproduced and presence or absence of digital output into user setting part
A402
Transmit start command, title, and presence or absence of digital output
A403
End
A404

Fig.12

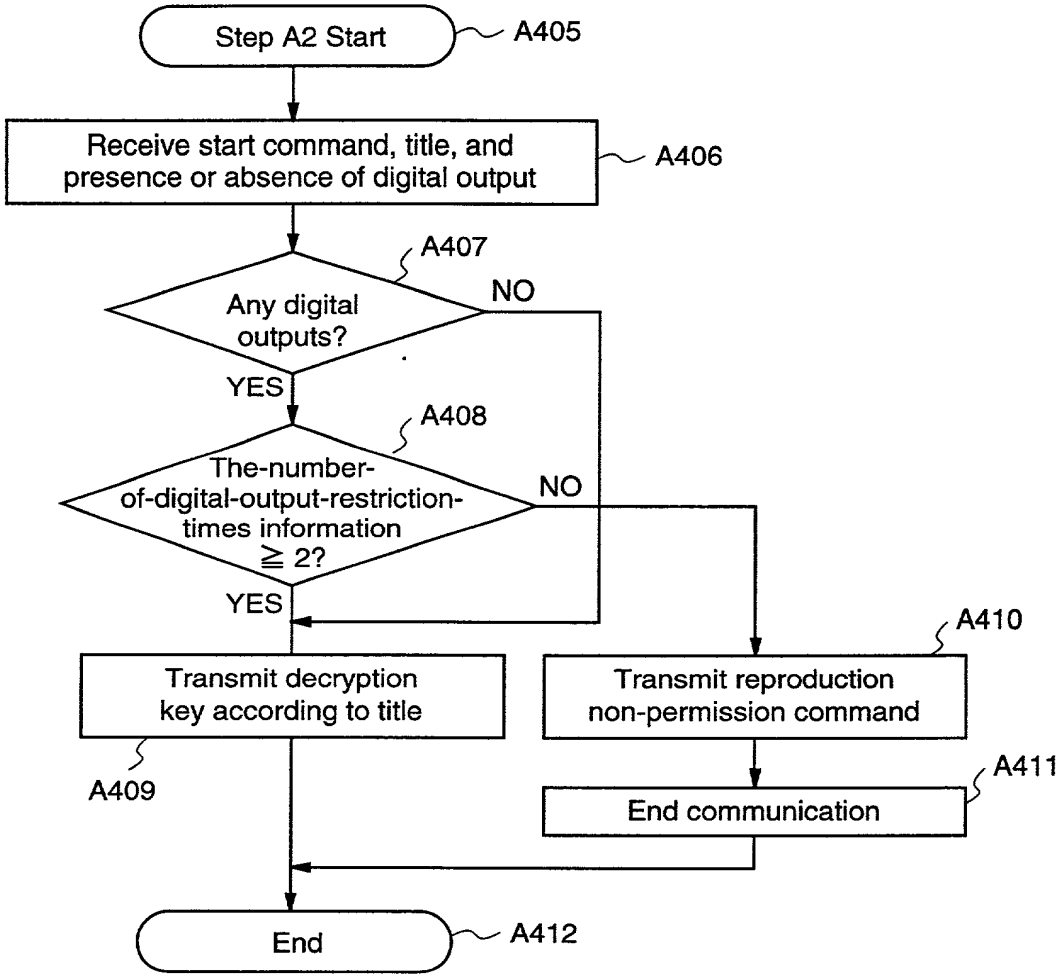

Step A2 Start
A405
Receive start command, title, and presence or absence of digital output
A406
A407
Any digital outputs?
NO
YES
A408
The-number-of-digital-output-restriction-times information ≧ 2?
NO
YES
A410
Transmit decryption key according to title
Transmit reproduction non-permission command
A409
A411
End communication
End
A412

Fig.13

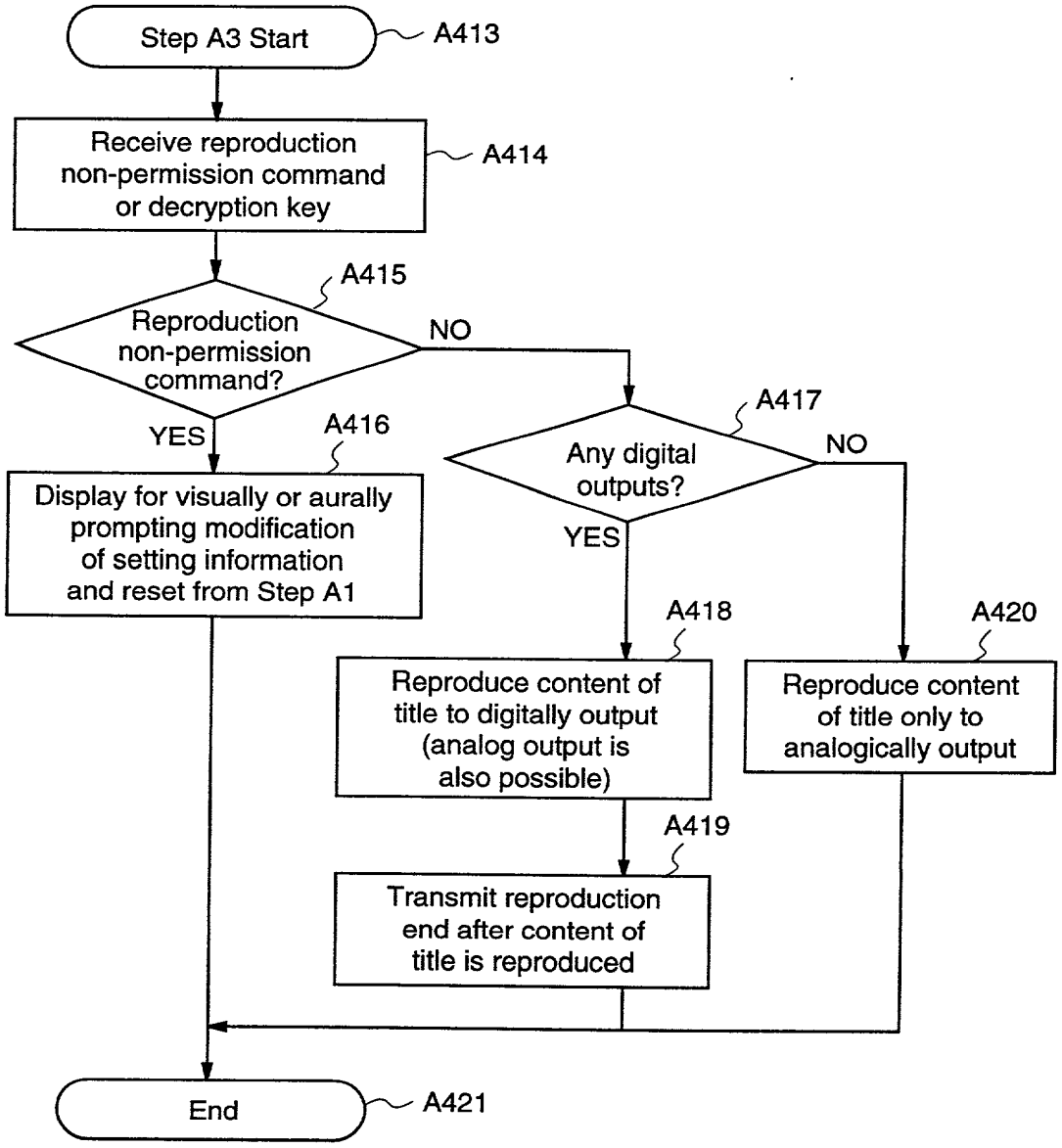

Step A3 Start
A413
Receive reproduction non-permission command or decryption key
A414
A415
Reproduction non-permission command?
NO
YES
A416
Display for visually or aurally prompting modification of setting information and reset from Step A1
A417
Any digital outputs?
NO
YES
A418
Reproduce content of title to digitally output (analog output is also possible)
A419
Transmit reproduction end after content of title is reproduced
A420
Reproduce content of title only to analogically output
End
A421

Fig.14

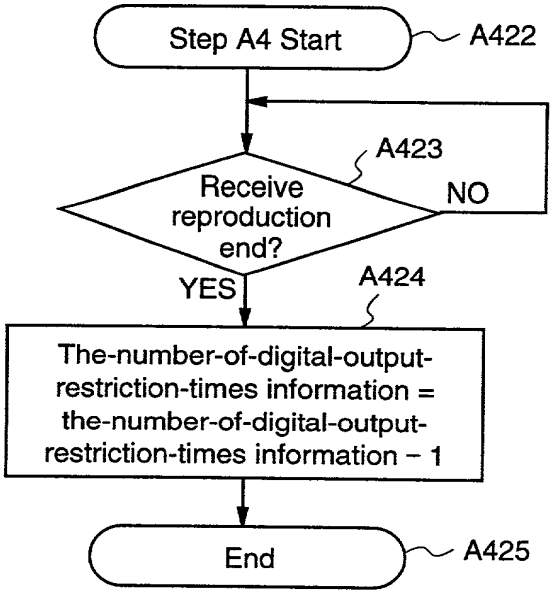
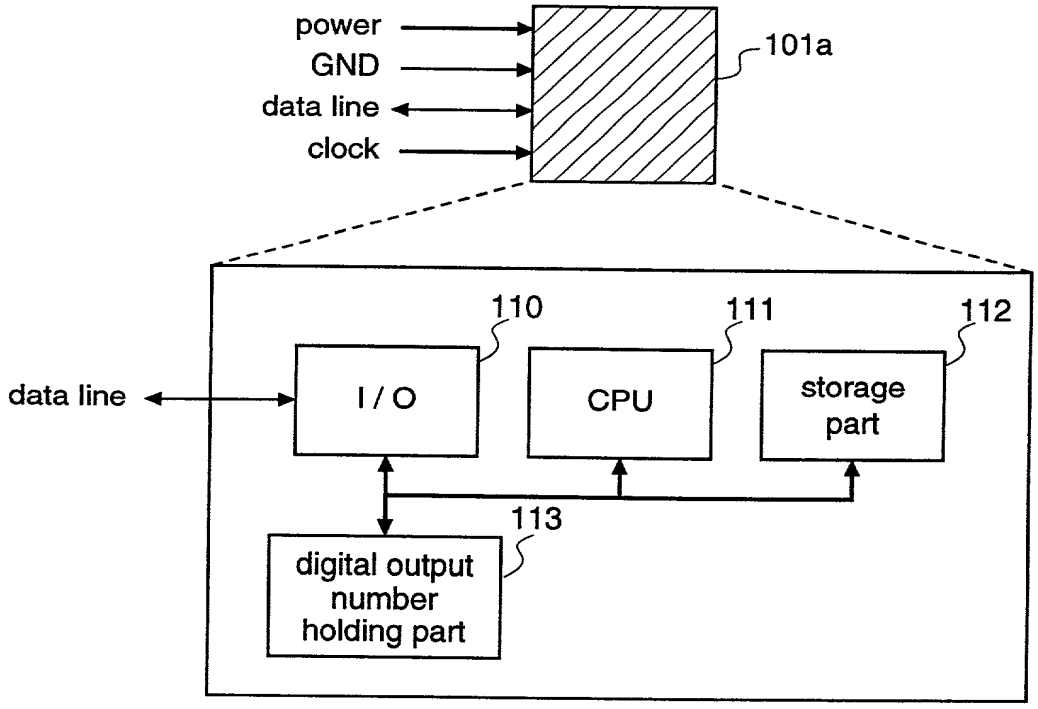

Step A4 Start
A422
A423
Receive reproduction end?
NO
YES
A424
The-number-of-digital-output-restriction-times information = the-number-of-digital-output-restriction-times information − 1
End
A425

Fig.15


power
GND
data line
clock
101a
110
111
112
data line
I / O
CPU
storage part
113
digital output number holding part

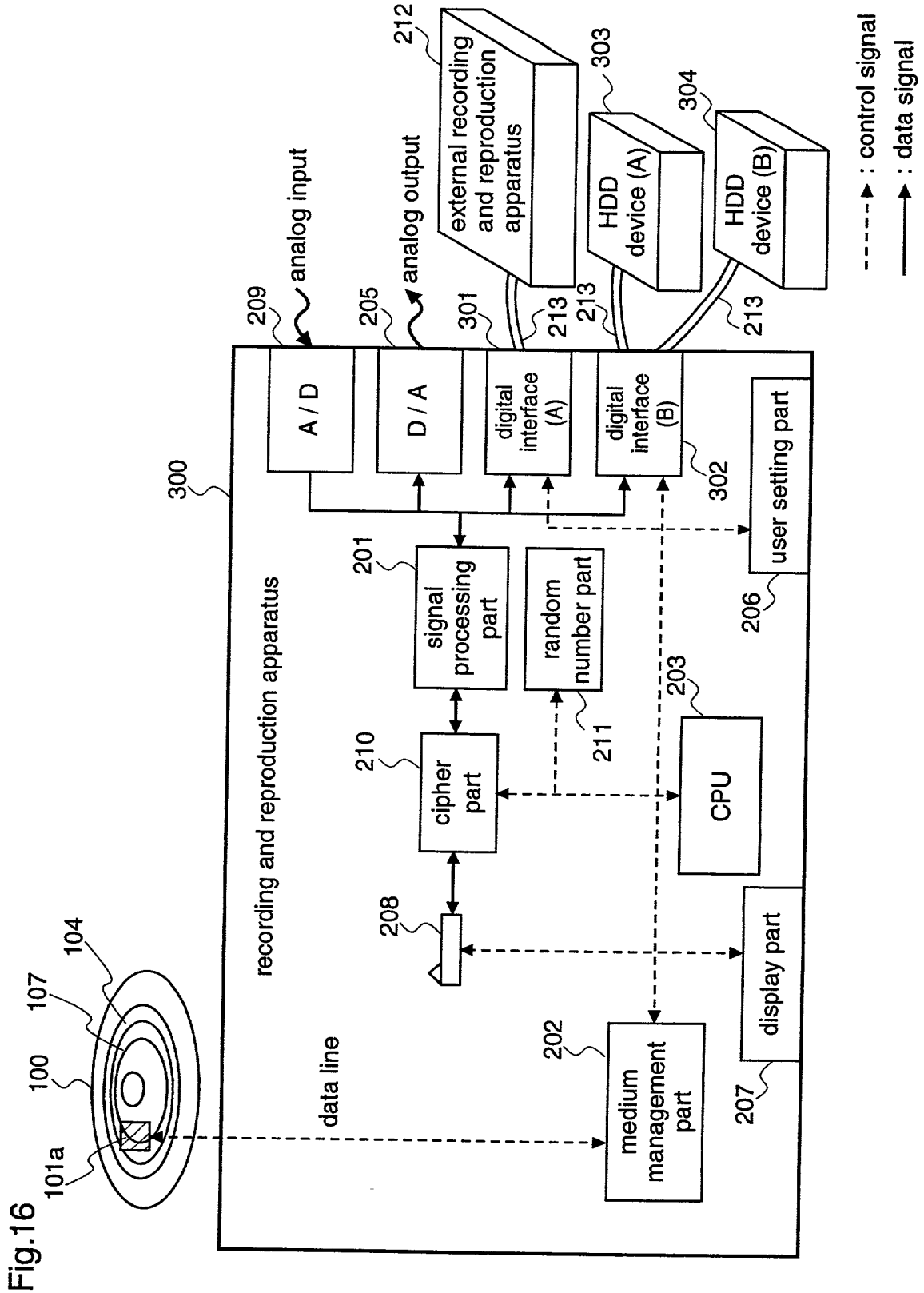

recording and reproduction apparatus
300
A / D
D / A
digital interface (A)
digital interface (B)
user setting part
signal processing part
random number part
cipher part
CPU
medium management part
display part
data line
analog input
analog output
external recording and reproduction apparatus
HDD device (A)
HDD device (B)
209
205
301
213
212
303
304
302
201
206
210
211
203
208
202
207
104
107
100
101a
: control signal
: data signal

Fig.16

Fig.17

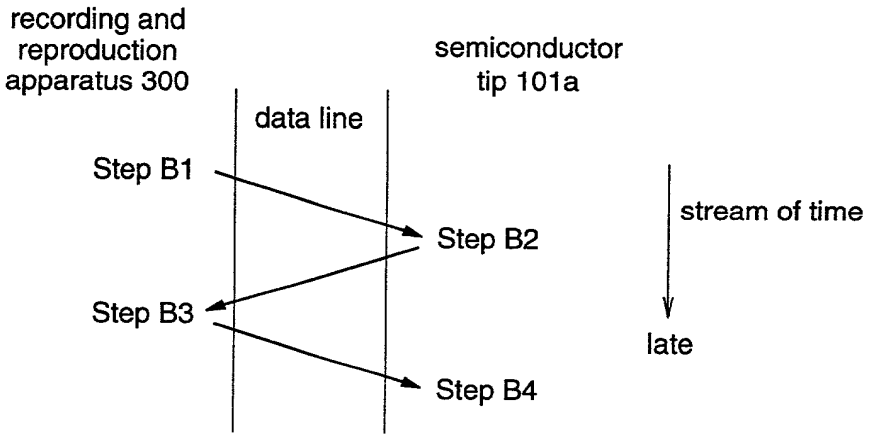

recording and reproduction apparatus 300
semiconductor tip 101a
data line
Step B1
Step B2
Step B3
Step B4
stream of time
late

Fig.18

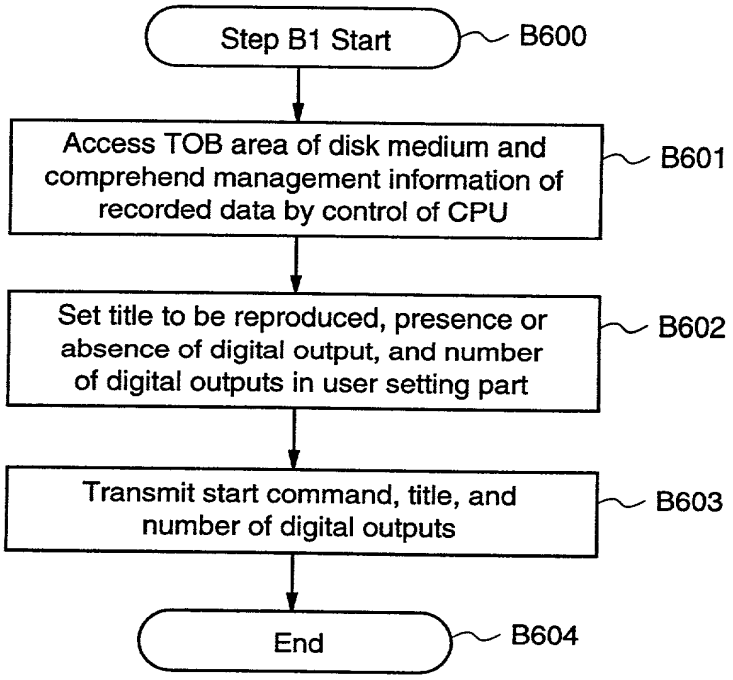

Step B1 Start
B600
Access TOB area of disk medium and comprehend management information of recorded data by control of CPU
B601
Set title to be reproduced, presence or absence of digital output, and number of digital outputs in user setting part
B602
Transmit start command, title, and number of digital outputs
B603
End
B604

Fig.19

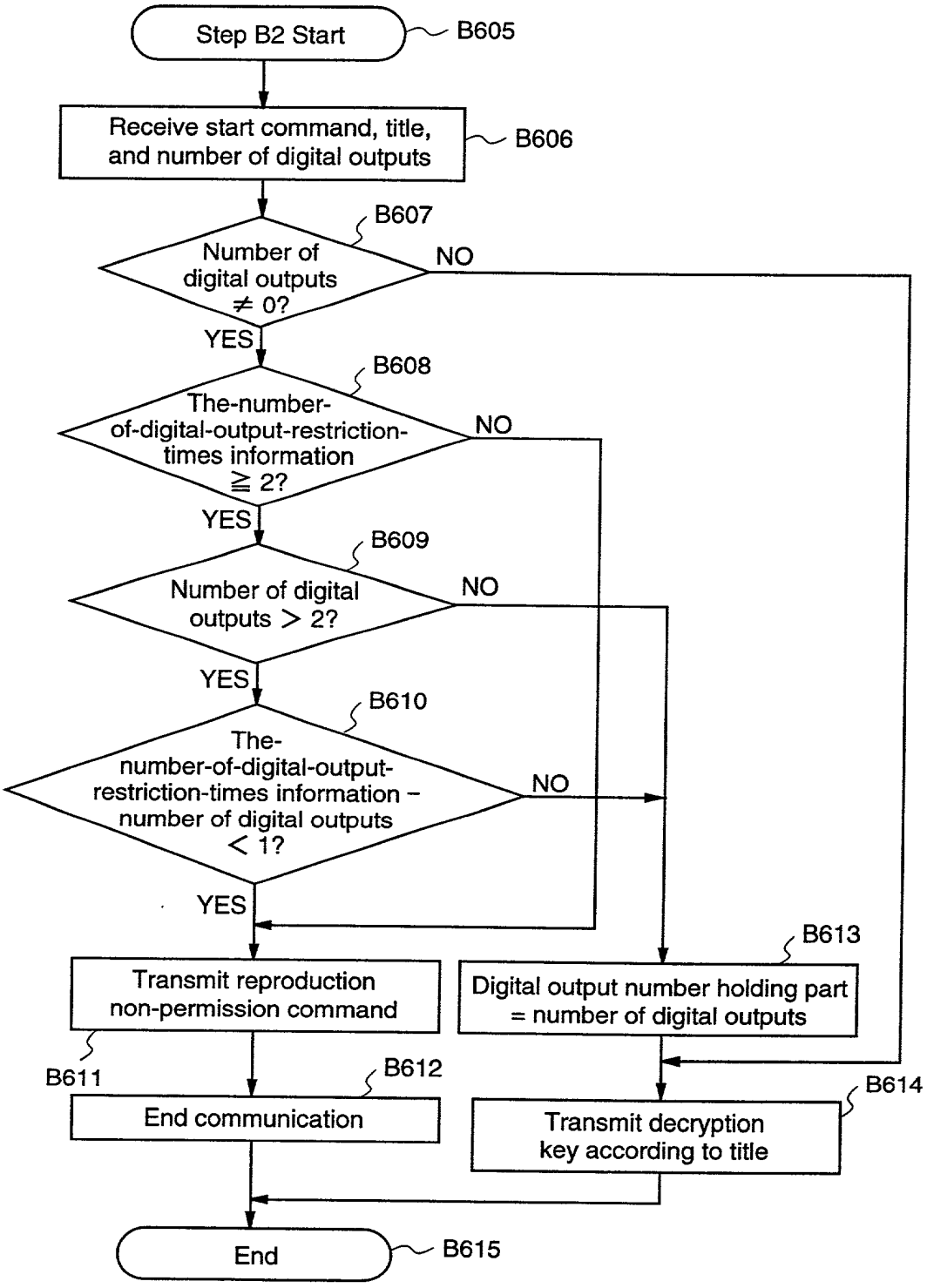

Step B2 Start
B605
Receive start command, title, and number of digital outputs
B606
B607
Number of digital outputs ≠ 0?
NO
YES
B608
The-number-of-digital-output-restriction-times information ≧ 2?
NO
YES
B609
Number of digital outputs > 2?
NO
YES
B610
The-number-of-digital-output-restriction-times information − number of digital outputs < 1?
NO
YES
B613
Transmit reproduction non-permission command
Digital output number holding part = number of digital outputs
B611
B612
End communication
B614
Transmit decryption key according to title
End
B615

Fig.20

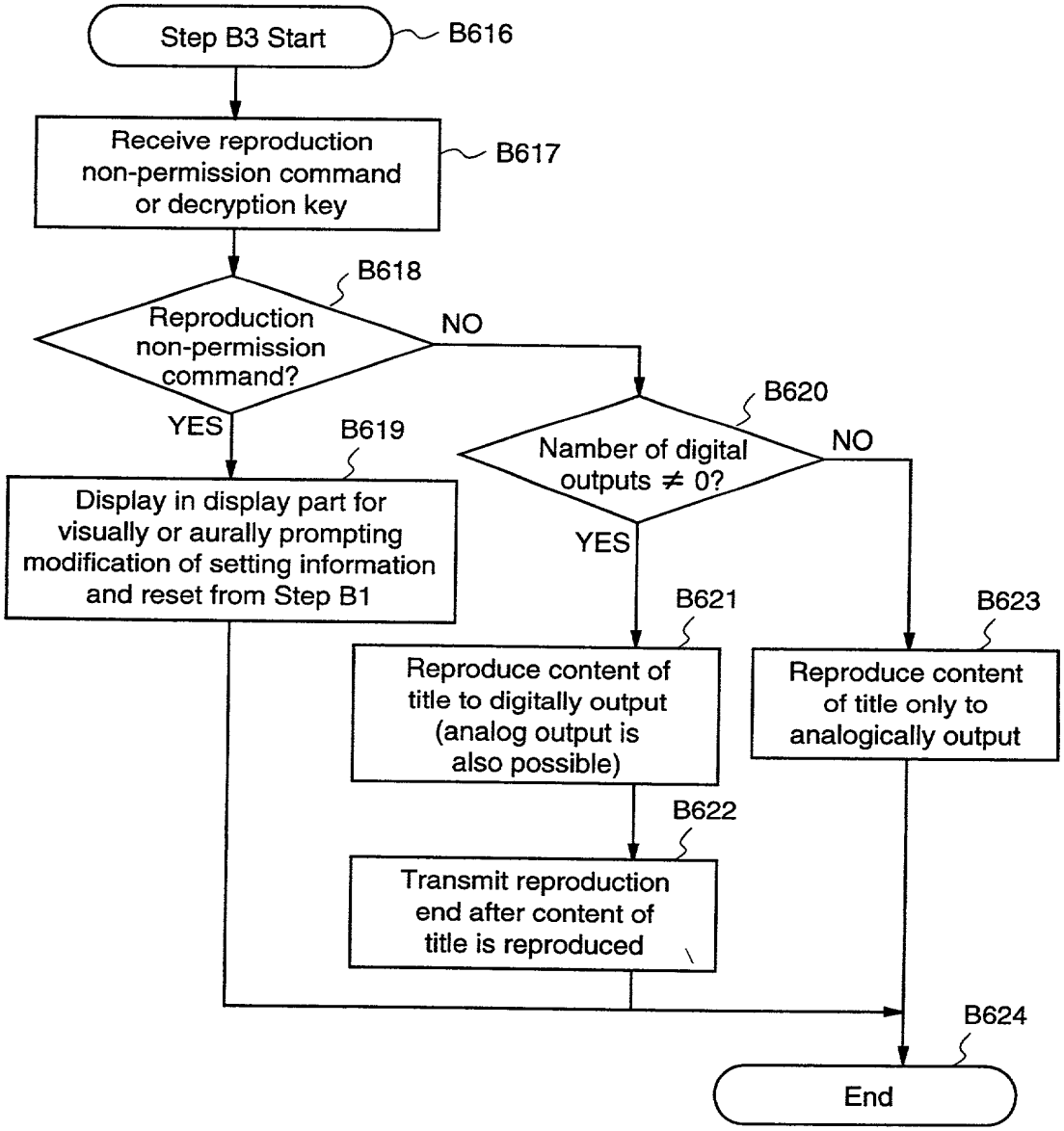

Step B3 Start
B616
Receive reproduction non-permission command or decryption key
B617
B618
Reproduction non-permission command?
NO
YES
B619
Display in display part for visually or aurally prompting modification of setting information and reset from Step B1
B620
Namber of digital outputs ≠ 0?
NO
YES
B621
Reproduce content of title to digitally output (analog output is also possible)
B622
Transmit reproduction end after content of title is reproduced
B623
Reproduce content of title only to analogically output
B624
End

Fig.21

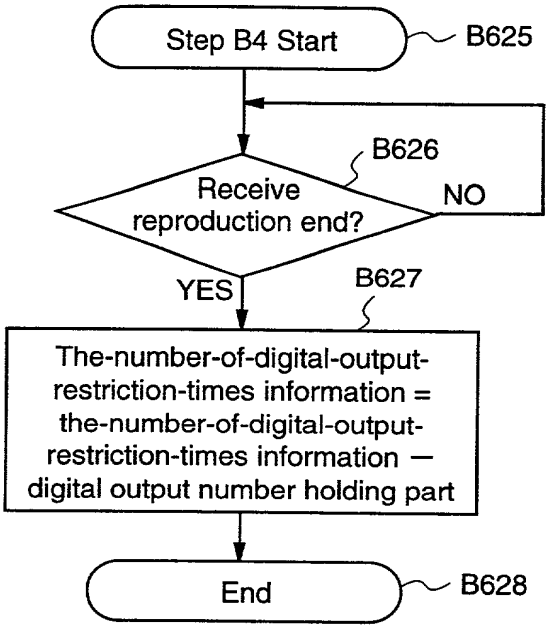

Step B4 Start
B625
B626
Receive reproduction end?
NO
YES
B627
The-number-of-digital-output-restriction-times information = the-number-of-digital-output-restriction-times information — digital output number holding part
End
B628

Fig.22

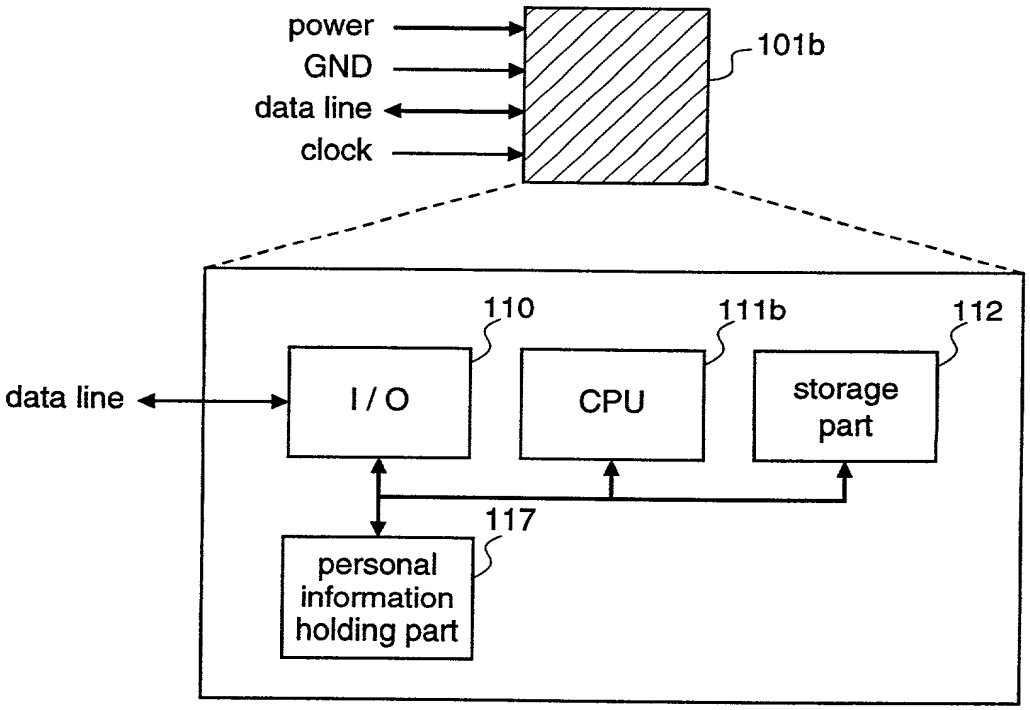

power
GND
data line
clock
101b
110
111b
112
data line
I / O
CPU
storage part
117
personal information holding part

Fig.23

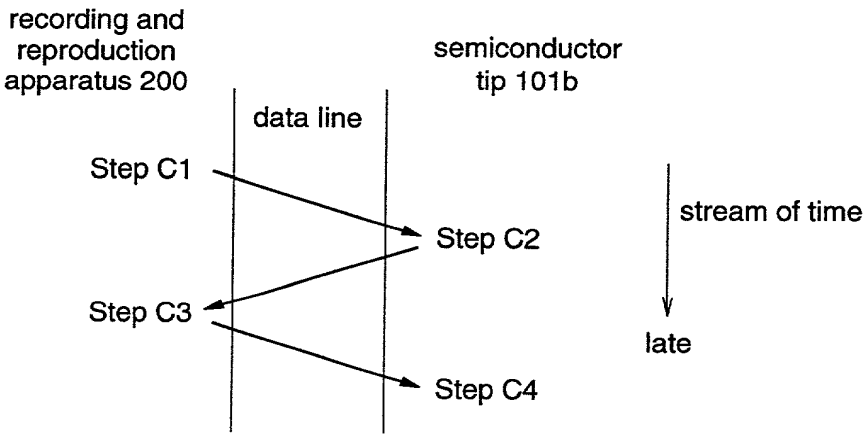

recording and reproduction apparatus 200
semiconductor tip 101b
data line
Step C1
Step C2
Step C3
Step C4
stream of time
late

Fig.24

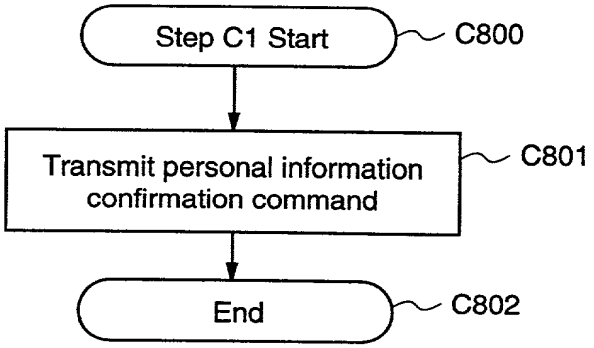

Step C1 Start
C800
Transmit personal information confirmation command
C801
End
C802

Fig.25

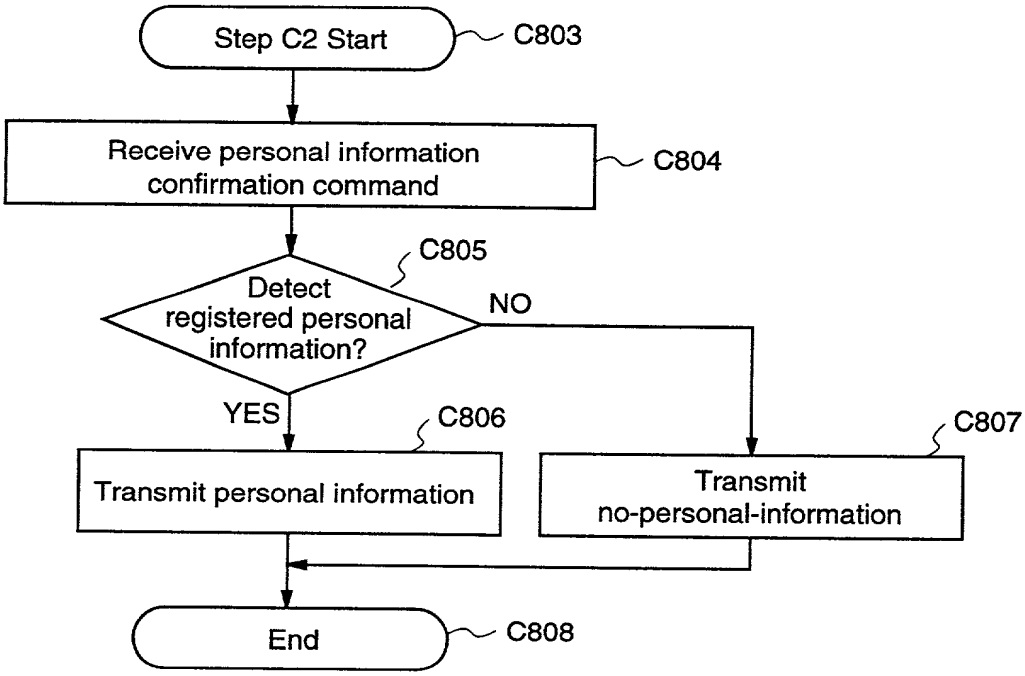

Step C2 Start
C803
Receive personal information confirmation command
C804
C805
Detect registered personal information?
NO
YES
C806
Transmit personal information
C807
Transmit no-personal-information
End
C808

Fig.26

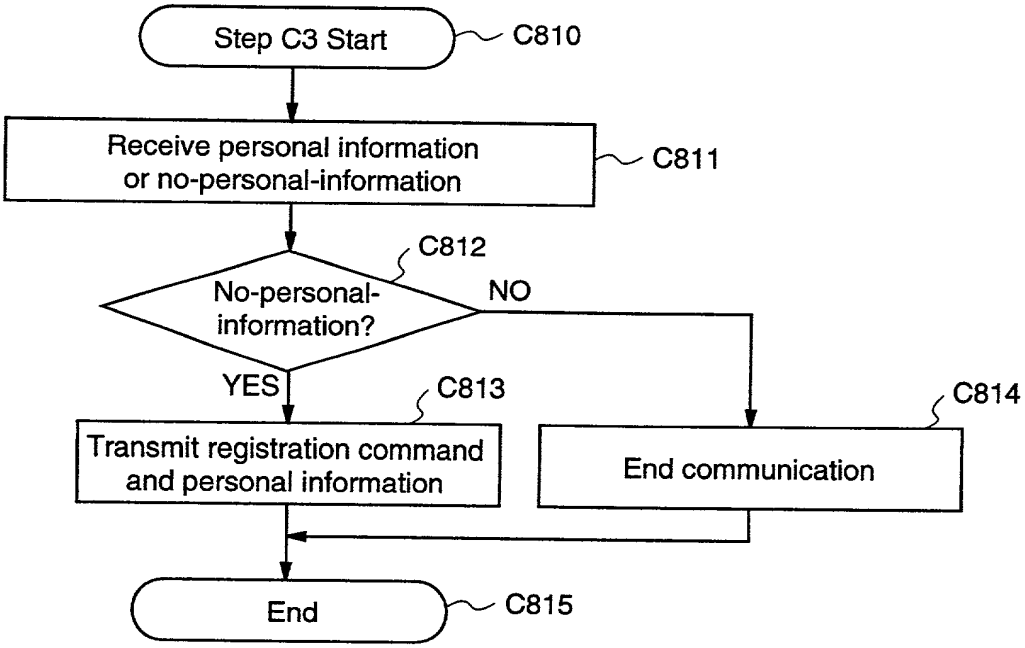

Step C3 Start
C810
Receive personal information or no-personal-information
C811
C812
No-personal-information?
NO
YES
C813
Transmit registration command and personal information
C814
End communication
End
C815

Fig.27

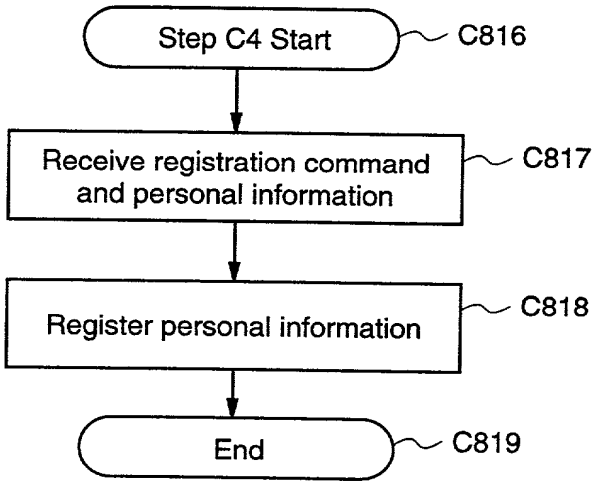

Step C4 Start
C816
Receive registration command and personal information
C817
Register personal information
C818
End
C819

Fig.28

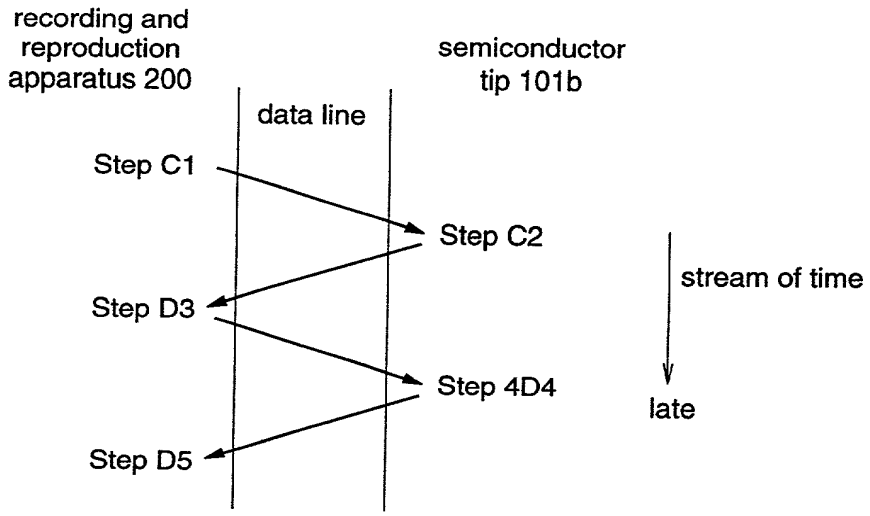

recording and reproduction apparatus 200
semiconductor tip 101b
data line
Step C1
Step C2
Step D3
Step 4D4
Step D5
stream of time
late

Fig.29

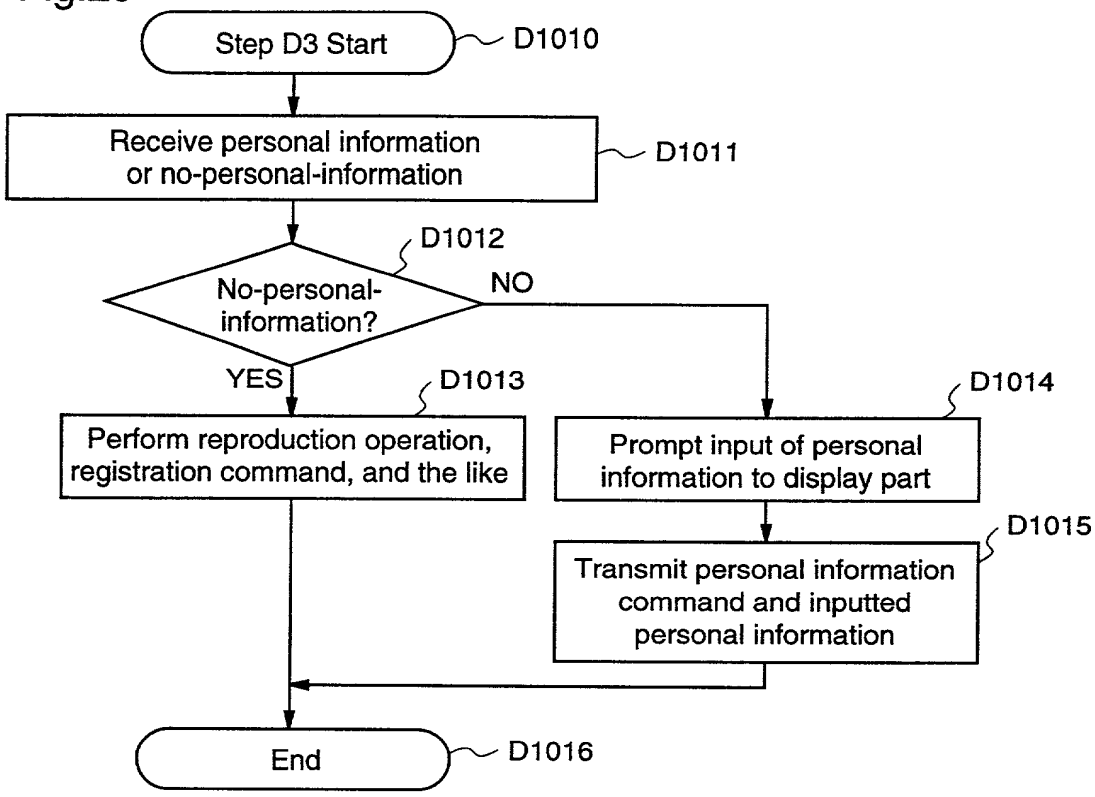

Step D3 Start
D1010
Receive personal information or no-personal-information
D1011
D1012
No-personal-information?
NO
YES
D1013
Perform reproduction operation, registration command, and the like
D1014
Prompt input of personal information to display part
D1015
Transmit personal information command and inputted personal information
End
D1016

Fig.30

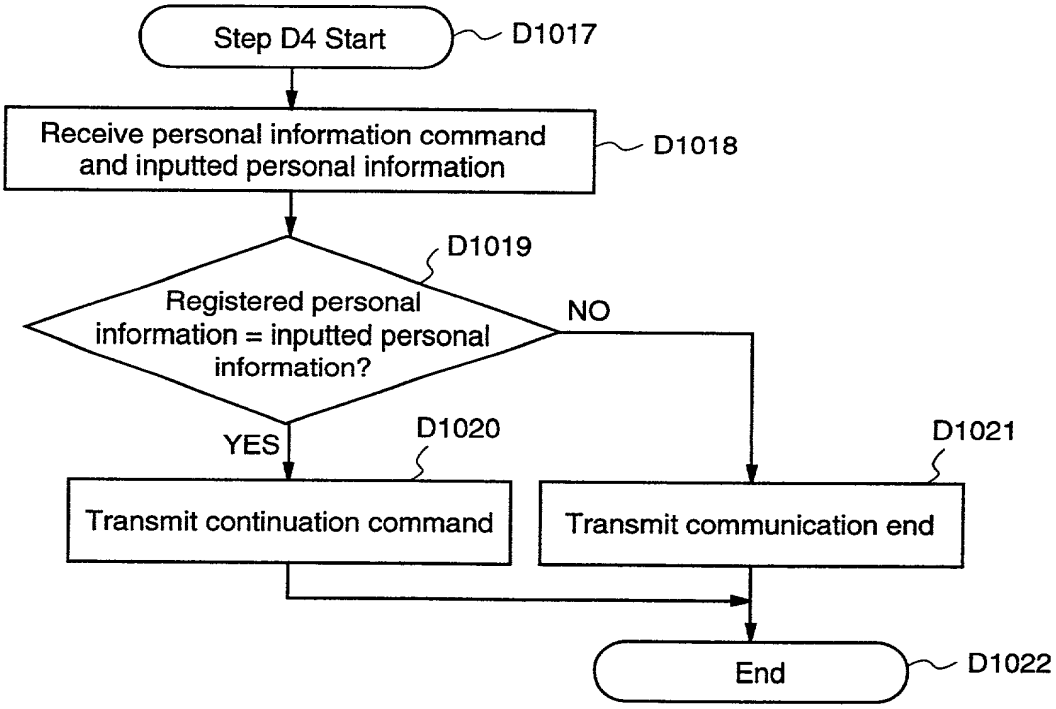

Step D4 Start
D1017
Receive personal information command and inputted personal information
D1018
D1019
Registered personal information = inputted personal information?
NO
YES
D1020
Transmit continuation command
D1021
Transmit communication end
End
D1022

Fig.31

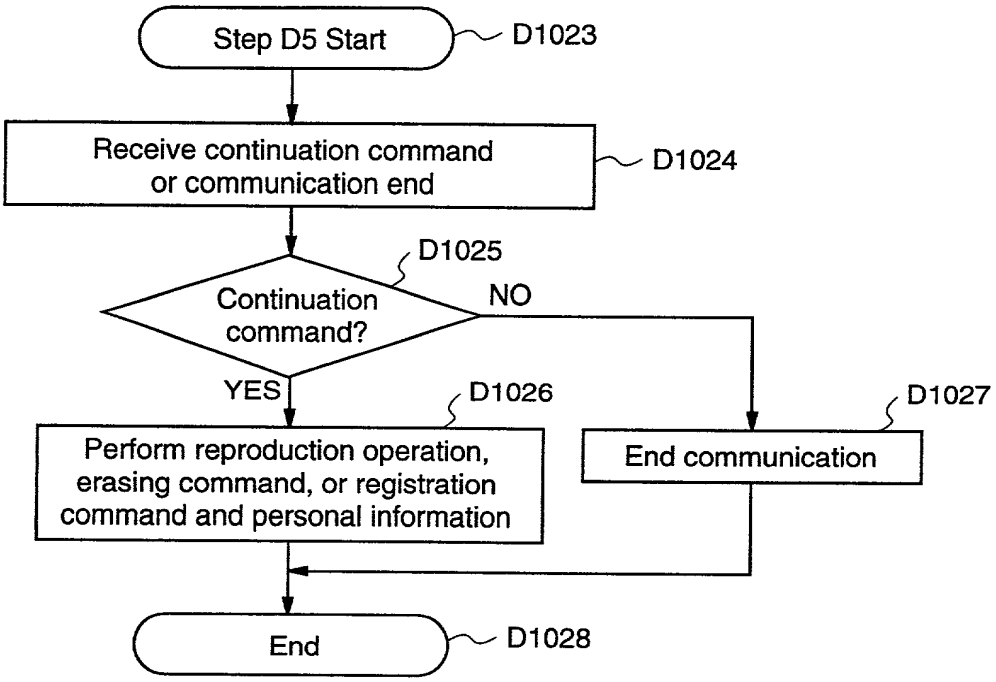

Step D5 Start
D1023
Receive continuation command or communication end
D1024
D1025
Continuation command?
NO
YES
D1026
Perform reproduction operation, erasing command, or registration command and personal information
D1027
End communication
End
D1028

Fig.32

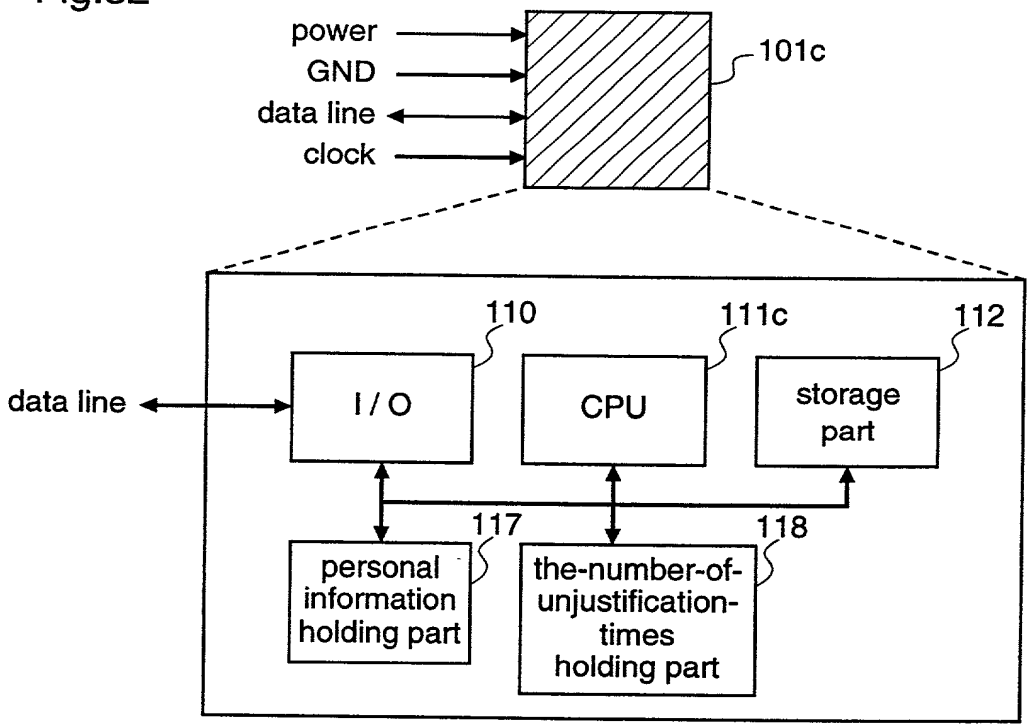

power
GND
data line
clock
101c
110
111c
112
data line
I / O
CPU
storage part
117
118
personal information holding part
the-number-of-unjustification-times holding part

Fig.33

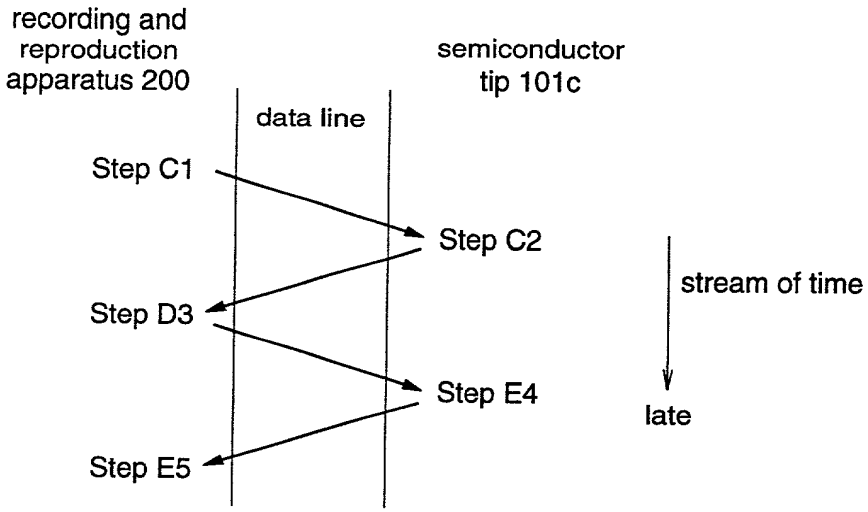

recording and reproduction apparatus 200
semiconductor tip 101c
data line
Step C1
Step C2
Step D3
Step E4
Step E5
stream of time
late

Fig.34

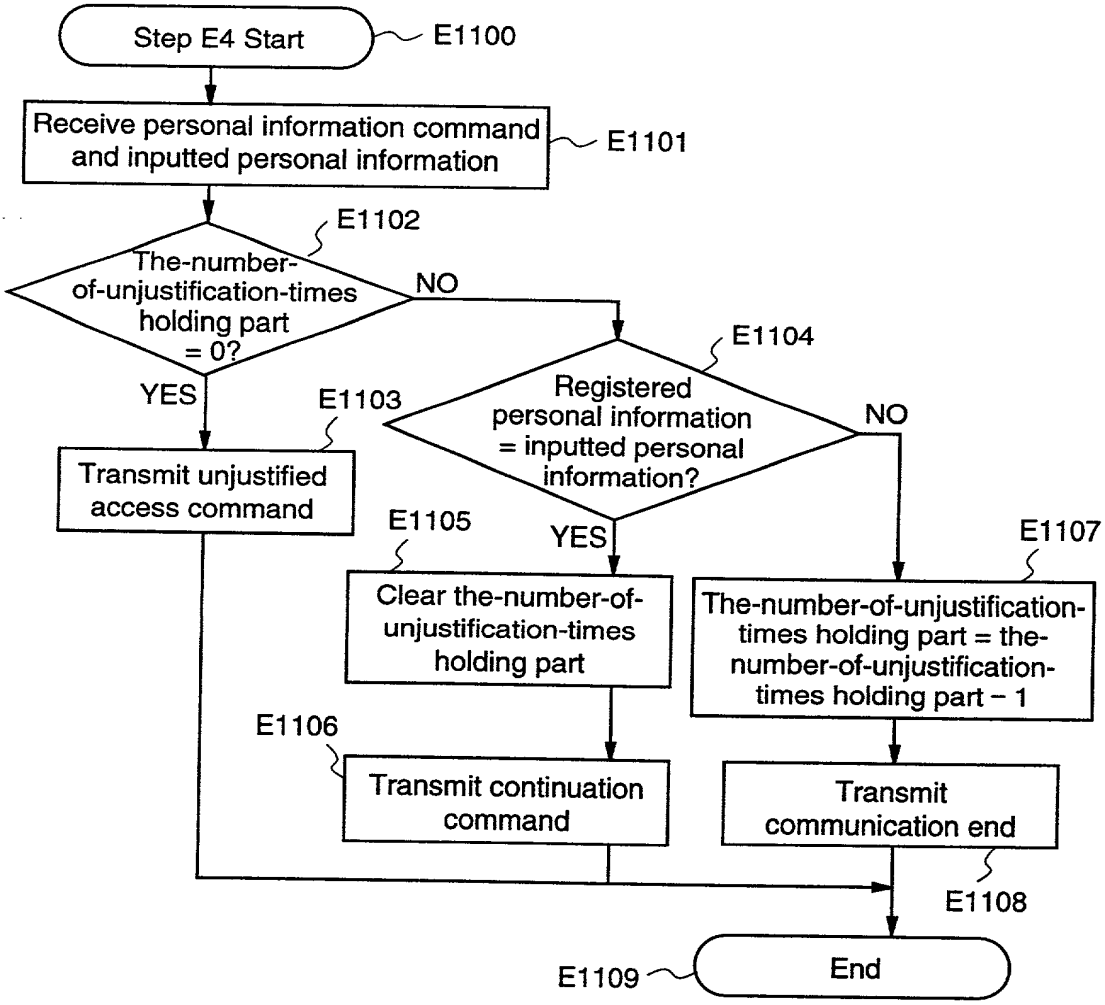

Step E4 Start
E1100
Receive personal information command and inputted personal information
E1101
E1102
The-number-of-unjustification-times holding part = 0?
NO
YES
E1103
Transmit unjustified access command
E1104
Registered personal information = inputted personal information?
NO
YES
E1105
Clear the-number-of-unjustification-times holding part
E1106
Transmit continuation command
E1107
The-number-of-unjustification-times holding part = the-number-of-unjustification-times holding part − 1
Transmit communication end
E1108
E1109
End

Fig.35

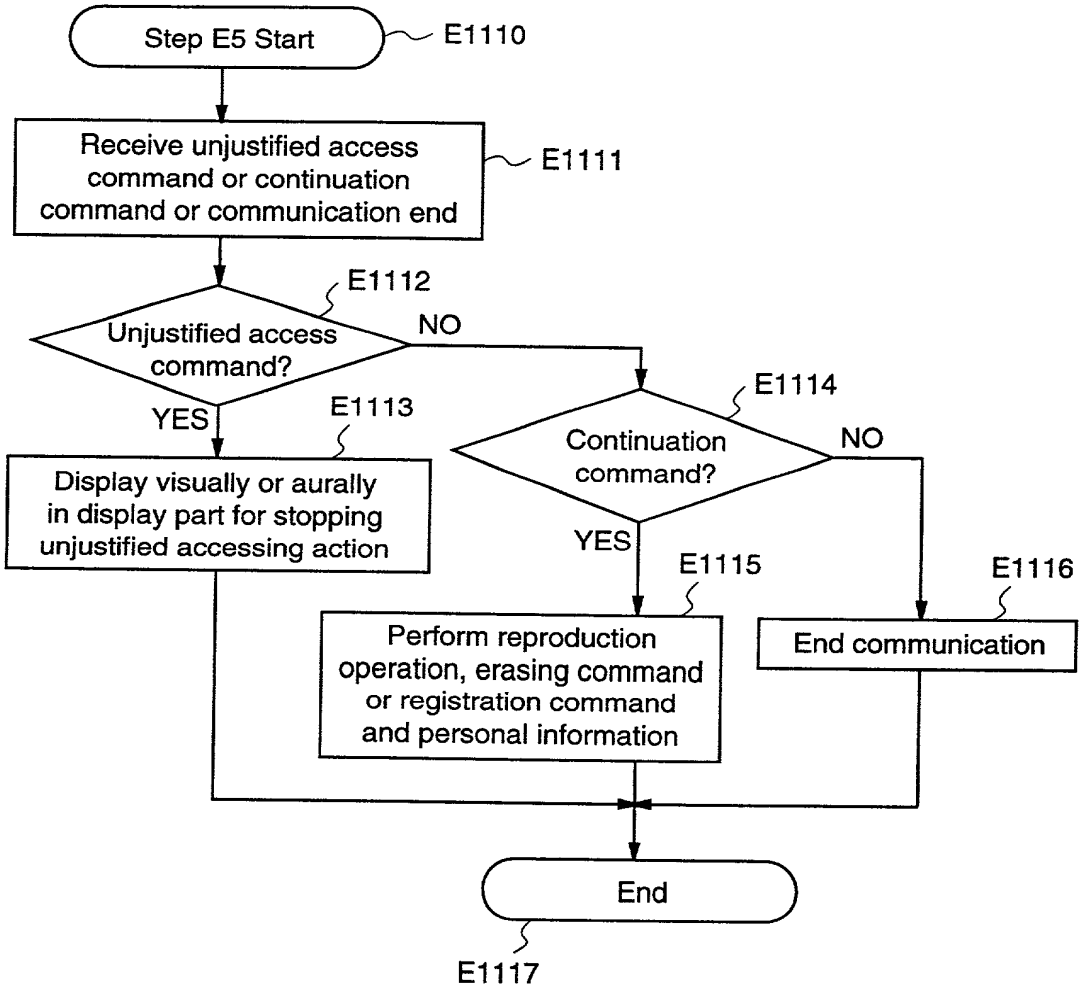
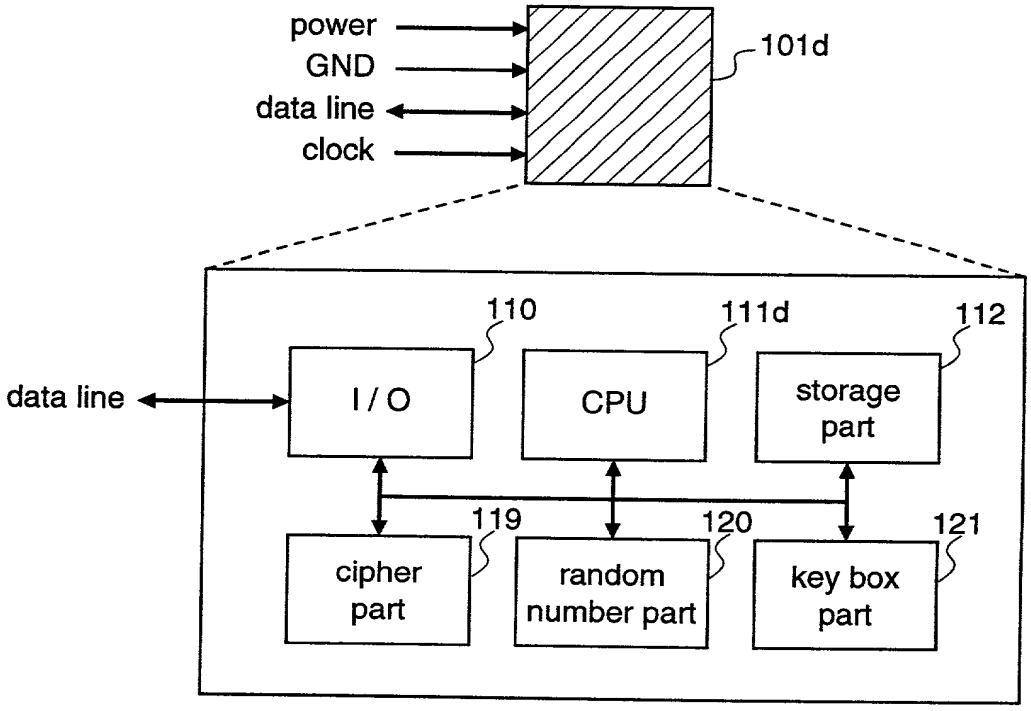

Step E5 Start
E1110
Receive unjustified access command or continuation command or communication end
E1111
E1112
Unjustified access command?
NO
YES
E1113
Display visually or aurally in display part for stopping unjustified accessing action
E1114
Continuation command?
NO
YES
E1115
Perform reproduction operation, erasing command or registration command and personal information
E1116
End communication
End
E1117

Fig.36


power
GND
data line
clock
101d
110
111d
112
data line
I / O
CPU
storage part
119
120
121
cipher part
random number part
key box part

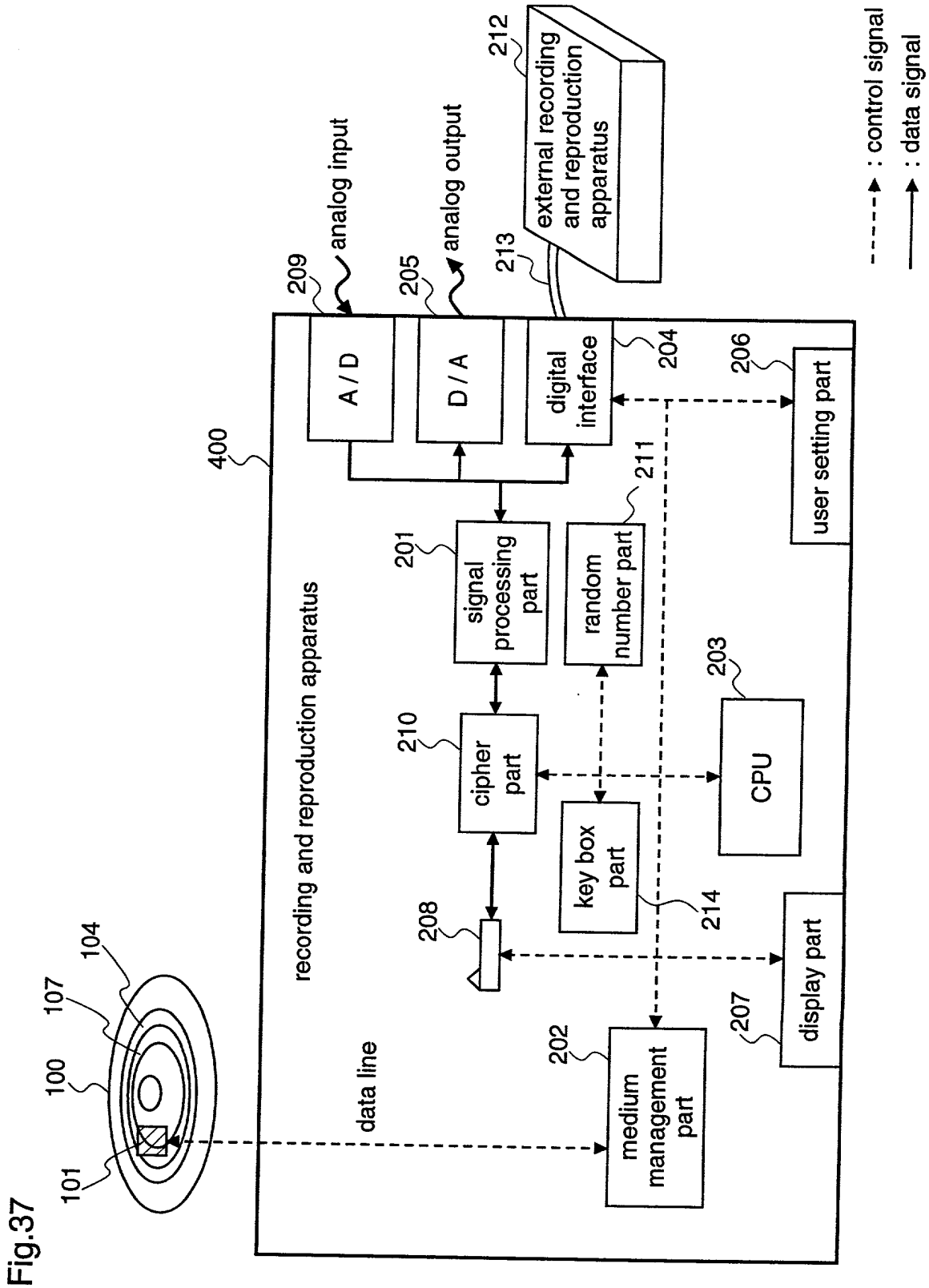

: control signal
: data signal
recording and reproduction apparatus
400
A / D
D / A
digital interface
204
analog input
209
analog output
205
212
external recording and reproduction apparatus
213
206
user setting part
211
random number part
201
signal processing part
203
CPU
210
cipher part
key box part
214
208
display part
207
202
medium management part
data line
100
101
104
107

Fig.37

Fig.38

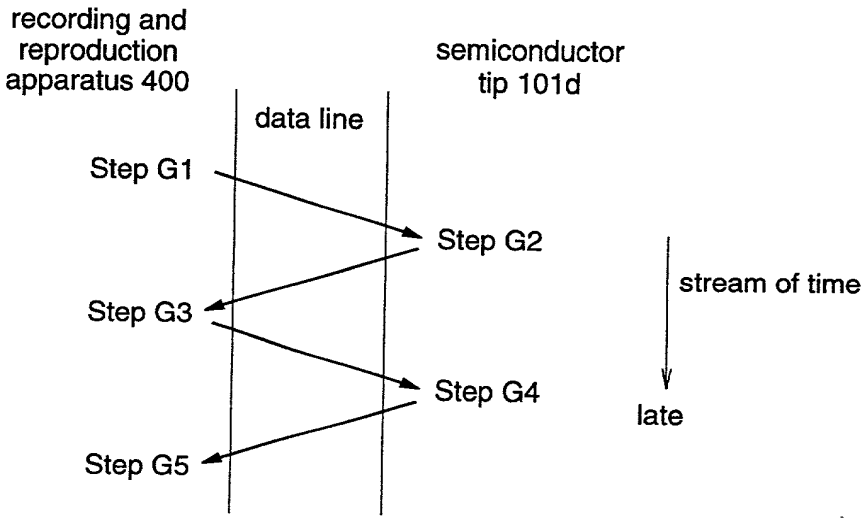

recording and reproduction apparatus 400
semiconductor tip 101d
data line
Step G1
Step G2
Step G3
Step G4
Step G5
stream of time
late

Fig.39

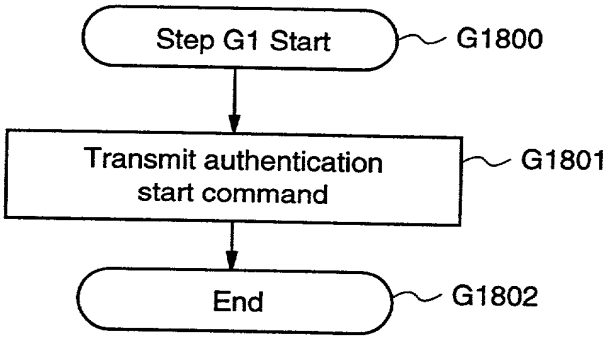

Step G1 Start
G1800
Transmit authentication start command
G1801
End
G1802

Fig.40

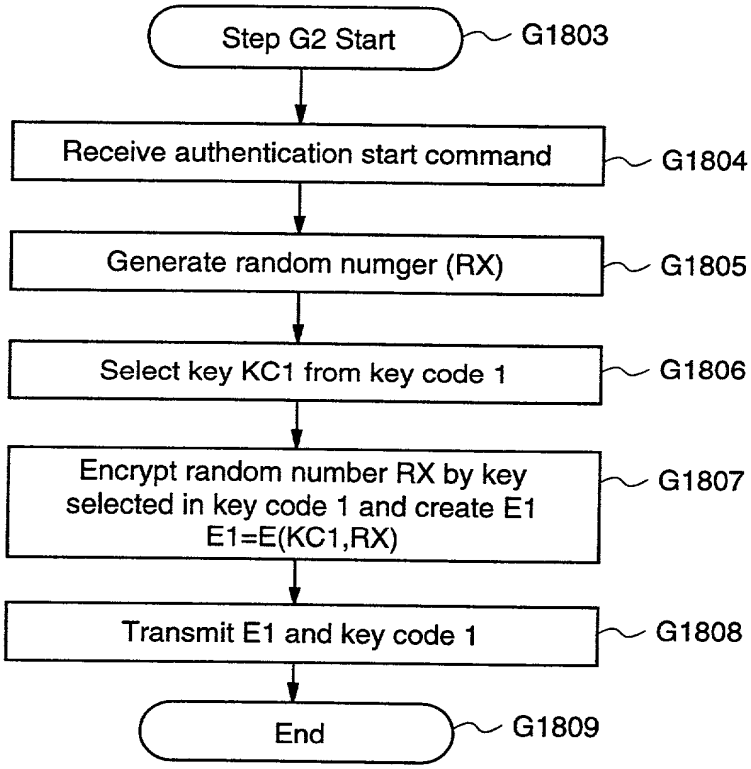

Step G2 Start
G1803
Receive authentication start command
G1804
Generate random numger (RX)
G1805
Select key KC1 from key code 1
G1806
Encrypt random number RX by key selected in key code 1 and create E1
E1=E(KC1,RX)
G1807
Transmit E1 and key code 1
G1808
End
G1809

Fig.41

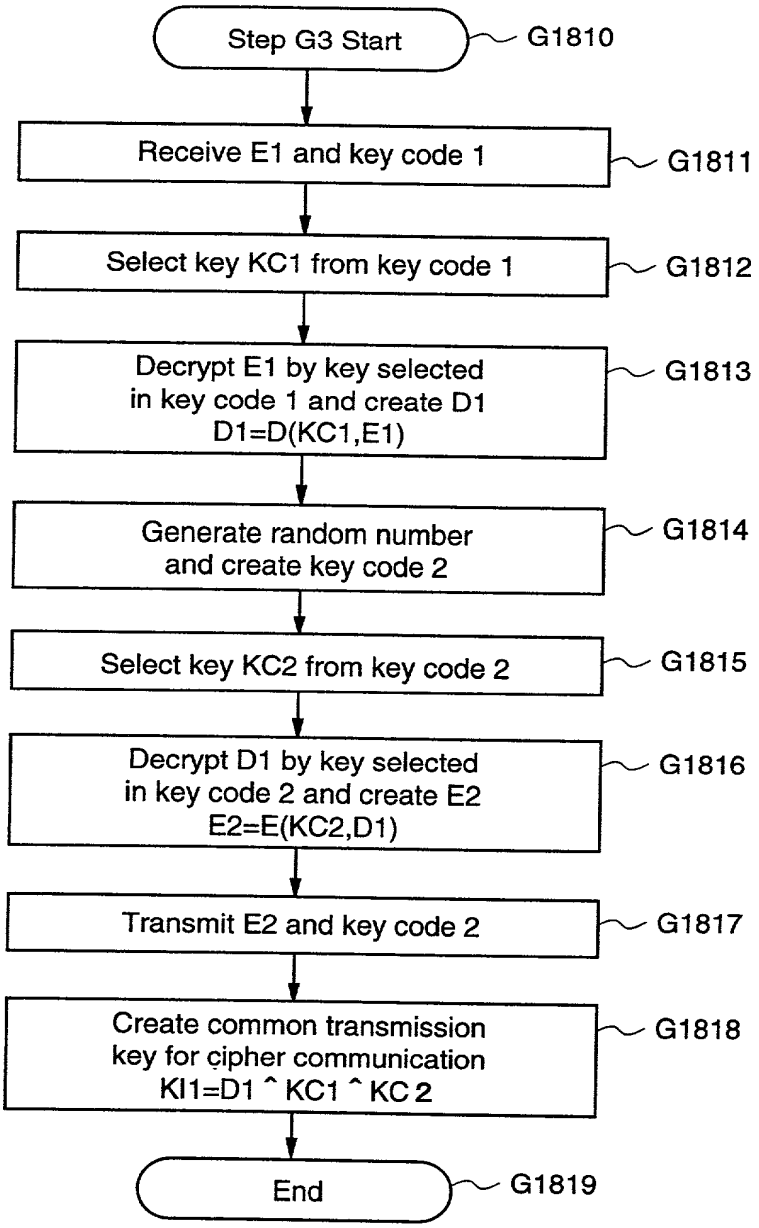

Step G3 Start
G1810
Receive E1 and key code 1
G1811
Select key KC1 from key code 1
G1812
Decrypt E1 by key selected in key code 1 and create D1 D1=D(KC1,E1)
G1813
Generate random number and create key code 2
G1814
Select key KC2 from key code 2
G1815
Decrypt D1 by key selected in key code 2 and create E2 E2=E(KC2,D1)
G1816
Transmit E2 and key code 2
G1817
Create common transmission key for cipher communication KI1=D1 ^ KC1 ^ KC 2
G1818
End
G1819

Fig.42

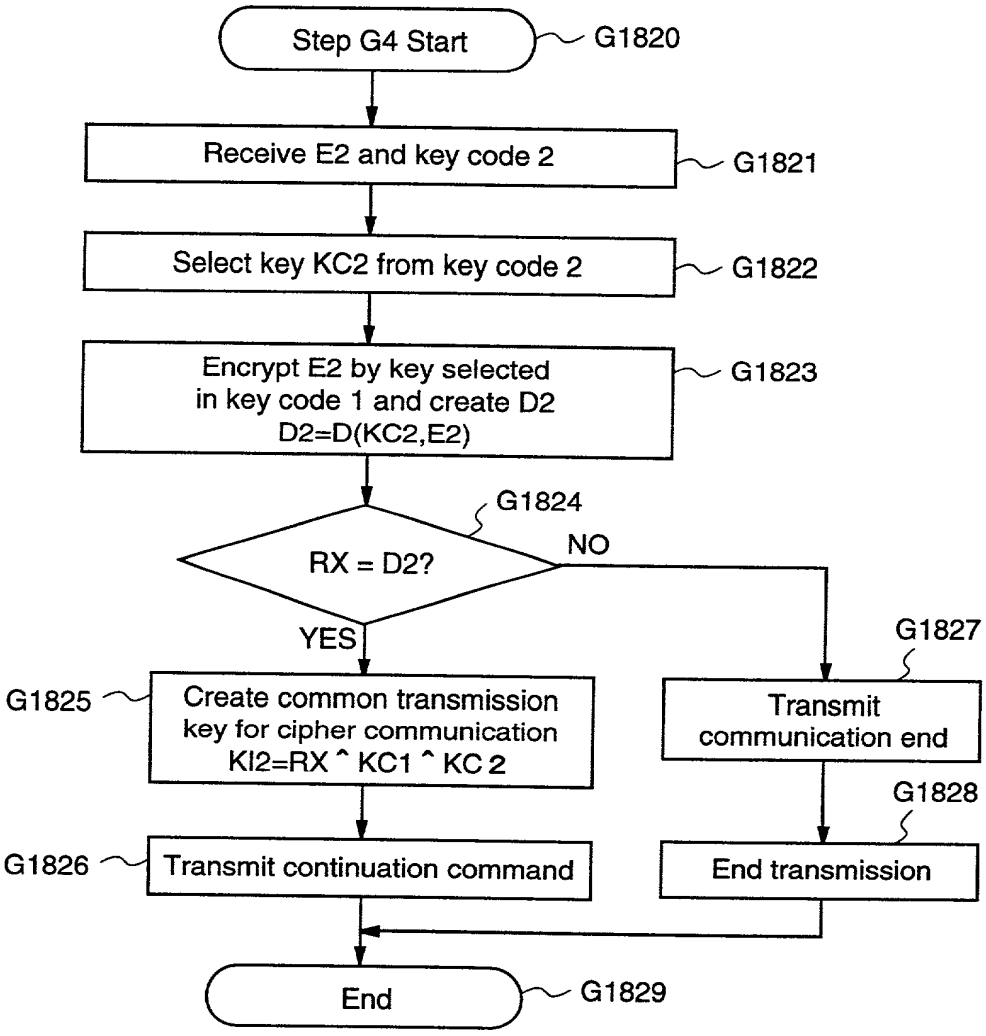

Step G4 Start
G1820
Receive E2 and key code 2
G1821
Select key KC2 from key code 2
G1822
Encrypt E2 by key selected in key code 1 and create D2
D2=D(KC2,E2)
G1823
G1824
RX = D2?
NO
YES
G1827
G1825
Create common transmission key for cipher communication
KI2=RX ^ KC1 ^ KC 2
Transmit communication end
G1828
G1826
Transmit continuation command
End transmission
End
G1829

Fig.43

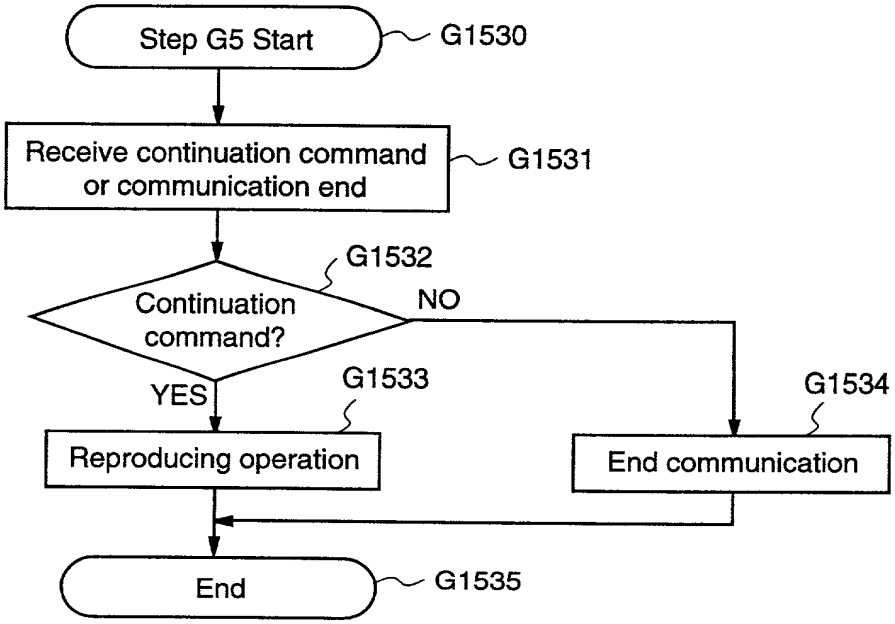


Fig.44

Free	copy free
Never Copy	no copy
One More Copy	only one more copy possible
No More Copy	no copy (No More Copy, when a content of One More Copy is recorded on a different medium)

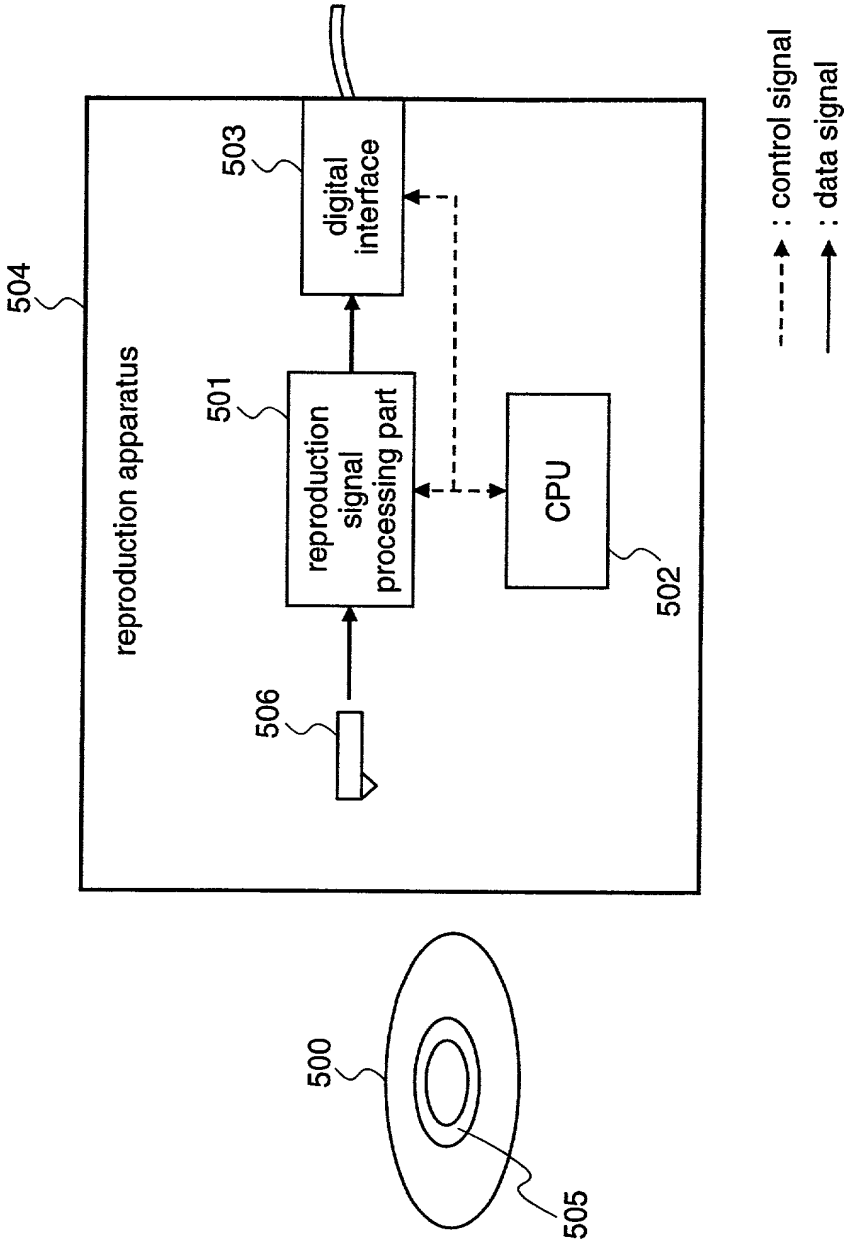

504
reproduction apparatus
503
digital interface
501
reproduction signal processing part
CPU
502
506
500
505
: control signal
: data signal

Fig.45

Declaration and Power of Attorney Under Patent Cooperation Treaty 35 USC §371(c)(4)

As a below-named inventor, I hereby declare that:

my residence, post office address and citizenship are as stated below next to my name; that

I verily believe that I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural names are named below) of the invention entitled: DATA RECORDING MEDIUM AND DATA MANAGEMENT SYSTEM

described and claimed in the international application number PCT/JP00/03482 filed May 31, 2000 and as amended on _____ (if any), the specification and claims of which I have reviewed and understand and for which I solicit a patent.

I acknowledge my duty to disclose information of which I am aware which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a), and that no application for patent or inventor's certificate on this invention has been filed in any country foreign to the United States of America prior to my international application by me or my legal representatives or assigns, except as follows:

Japanese Patent Application No. 11-152057 filed May 31, 1999

The priority of the above applications (if any), filed within a year prior to my international application is hereby claimed under 35 USC 119. I hereby appoint the following as my attorneys of record with full power of substitution and revocation to prosecute this application and to transact all business in the patent office:

Roger W. Parkhurst, Reg. No. 25,177; Charles A. Wendel, Reg. No. 24,453

ALL CORRESPONDENCE IN CONNECTION WITH THIS APPLICATION SHOULD BE SENT TO: PARKHURST & WENDEL, L.L.P., 1421 PRINCE STREET, SUITE 210, ALEXANDRIA, VIRGINIA 22314-2805, TELEPHONE (703) 739-0220.

I hereby declare that I have reviewed and understand the contents of this Declaration, and that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

3. Full Name of Sole or First Inventor: Hiroshi (Given Name) | (Middle Initial) | KASHIWA (Family Name)

*4. Inventor's Signature: Hiroshi Kashiwa

Date of Signature: December 13, 2001 (Month / Day / Year)

6. Residence: Itami-shi (City) | (State or Province) | Japan (Country)

7. Citizenship: Japanese

8. Post Office address (Insert complete mailing address, including country): 348-1-702, Ikejiri 2-chome, Itami-shi, Hyogo 664-0027 Japan

*IF THERE IS MORE THAN ONE INVENTOR USE PAGE 2 AND PLACE AN "X" HERE☐.